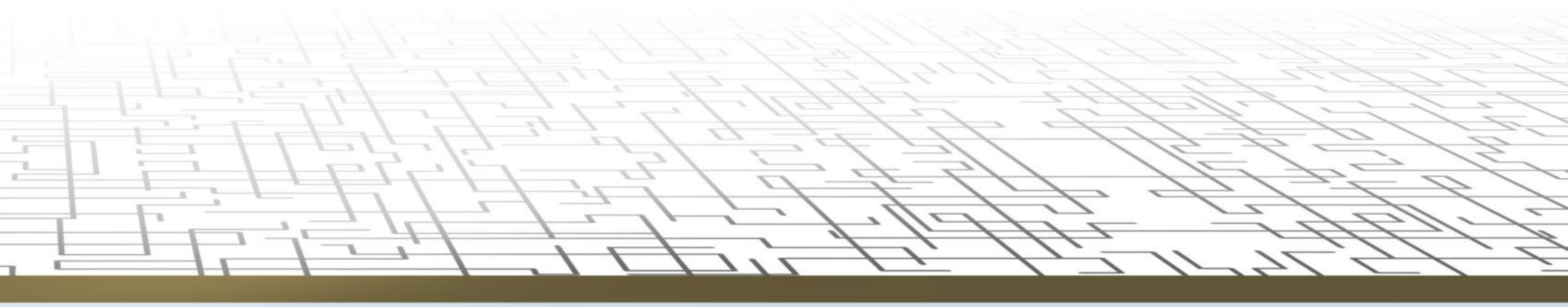
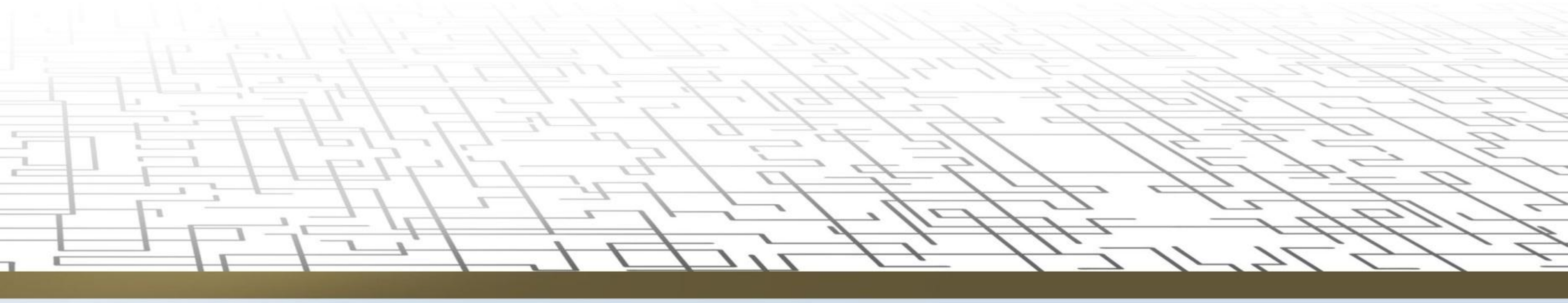


INFORMATION SHARING ENVIRONMENT

INFORMATION INTEROPERABILITY FRAMEWORK (I^2F)

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING



INFORMATION SHARING ENVIRONMENT

INFORMATION INTEROPERABILITY FRAMEWORK (I^2F)

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

VERSION 0.5

MARCH 2014

This page intentionally left blank.

DOCUMENT INFORMATION

Document Title	**Information Sharing Environment (ISE) Information Interoperability Framework (I^2F)**
Document Owner	Office of the Program Manager, Information Sharing Environment (PM-ISE)
Document Responsibility	PM-ISE
Document Version	0.5
Document Status	Delivered

DOCUMENT CHANGE HISTORY

Date	Version	Changed By	Change Description
16 May 2013	0.1	PM-ISE	Initial distribution of draft paper.
24 June 2013	0.2	PM-ISE	**Overall:** 1. Adjudicated comments of first draft IISC review. 2. Added table of contents. 3. Added descriptions of I^2F Components (Exchange Specifications, Technical Capabilities, Technical Capabilities, Exchange Patterns, and Technical Standards). 4. Aligned I^2F to Common Architecture Domains. 5. Added Exchange Patterns graphics and descriptions. **Appendix:** 6. Added existing Architecture Table Alignment – Grid.
16 August 2013	0.3	PM-ISE	**Overall:** 1. Adjudicated comments of second draft. 2. Added I^2F Landscape View, Common Profile, Standards and Specifications, and Architecture Framework Alignment. 3. Provided additional write-ups for I^2F Components. 4. Included Interoperability Reference Architecture Template draft. 5. Added Executive Summary. **Appendix:** 6. Added Standards Process and Governance, Common Profile, Authorities and References, Draft Glossary, Draft Use Case.
6 January 2014	0.4	PM-ISE	**Overall:** 1. Adjudicated comments of third draft. 2. Further Reconcile OMB, CIOC, NSISS strategies and policy in the I^2F. 3. Interface Elaborations and Descriptions updated. 4. I^2F Process Diagram and IDEF0 added. 5. Updated Reference Architecture Template and Use Case. 6. Added Interoperability Maturity Model. 7. Added Chapter 5: Building Interoperability into Mission-Based Architectures.

Date	Version	Changed By	Change Description
18 February 2014	0.5	PM-ISE	**Overall:** 1. Adjudicated January and February 2014 comments received from IISC and SCC. 2. Document name changed by Program Manager (PM) from ISE Interoperability Framework (I^{2}F) to *ISE Information Interoperability Framework (ISE I^{2}F)*. Document updated to include new name. 3. Official document overview provided to ISA IPC by PM, ISE (End of Phase 1).

FUTURE RELEASES

Date	Version	Proposed
March 2014	--	1. Incorporate MDA Interoperability Results. 2. Add documented concepts, tools techniques to the ISE website (Project Interoperability).

REVIEWERS AND CONTRIBUTORS

Agencies, Departments, and Organizations
American Council for Technology – Industry Advisory Council (ACT/IAC)
Department of Defense
Department of Homeland Security
Department of Justice
Department of State
Federal Bureau of Investigation
Georgia Tech Research Institute (GTRI)
Integrated Justice Information Systems (IJIS) Institute
Intelligence Communities
John Hopkins Applied Science Lab – Comprehensive National Cyber Initiative (CNCI-5)
National Information Exchange Model Program Management Office (NIEM PMO)
Object Management Group (OMG)
Organization for the Advancement of Structured Information Standards (OASIS)
Regional Information Sharing Systems (RISS)
Stanford University

CONTENTS

EXECUTIVE SUMMARY

BACKGROUND

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, called for the President to create an Information Sharing Environment (ISE) to share terrorism-related information among Federal, State, Local, and Tribal (SLT) governments; together with, where possible, private sector entities, and foreign partners.[1]

To assist in the development of the ISE, IRTPA 2004 provides for the designation of a program manager "responsible for information sharing across the Federal Government." The ISE requires responsible and accountable information sharing between the various Federal and SLT agencies. As such, the ISE represents a compelling tool in the continuing mission to detect and eliminate terrorist activities.

STRATEGIC APPROACH

Following the 2004 Act, The White House issued additional presidential directives called for development of an implementation plan showing how the proposed Information Sharing Environment could sustainably be built upon existing Federal resources. Once established, this implementation plan and the resultant integrated information sources can be examined using relevant data analysis techniques to detect relationships between things, people, places, and events and helping analysts to identify the connections between data that are not obviously related. This document, the ISE I^{2}F, builds on these strategies, tools, and directives to share information across multiple levels of government and non-government entities for the common good.[2] Successful implementation of this implementation plan requires commitment of planning from key stakeholders and communities of interest.

INTEROPERABILITY DEFINED

Information interoperability is defined in this document as "the ability to transfer and use information in a uniform and efficient manner across multiple organizations and information technology systems."[3,4] It is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.[5]

[1] http://www.house.gov/legcoun/Comps/IRTPA04.pdf

[2] EO 13356, http://www.fas.org/irp/offdocs/eo/eo-13356.htm, and EO 13388, https://www.fas.org/irp/offdocs/eo/eo-13388.htm.

[3] Australian Information Interoperability Framework, 2006.

[4] United States Code Title 44: Public Printing and Documents (2011) U.S.C. Title 44, Chap. 36, § 3601.

[5] *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries* (New York, NY: 1990).

From a technical perspective, interoperability is fostered through the consistent application of design principles and design standards to address a specific mission problem. This establishes an environment wherein services offered by disparate projects can be assembled into a variety of composition configurations to help automate a range of analytic tasks.[6] Goals of interoperability are discussed in Section 1.3.

OBJECTIVES

The ISE I^{2}F is used to guide the implementation of the ISE information sharing capabilities. The ISE approach links information across jurisdictional boundaries and creates a distributed, protected, trusted environment for sharing information. It provides mechanisms to permit partner agencies at the Federal, state, local, tribal, and territorial levels (e.g., fusion centers) to share similar data based on common standards and practices. The ISE I^{2}F exploits existing information architectures, suggesting standards, tools and methodologies to link existing systems as well as specifying the development of common artifacts that will enable disparate departments and agencies' architectures to make the full framework operational.

The ISE I^{2}F was developed so that ISE participants could better respond to complex policy challenges and improve the delivery of services and information to protect our citizens. To achieve a connected government, ISE participants require guidance to confidently manage, transfer, and exchange information by:

- Identifying key decision points for interoperability between disparate systems;
- Providing a comprehensive, high-level description of each interoperability domain; and,
- Establishing the framework for implementing ISE information sharing capabilities.

The ISE I^{2}F will accomplish the above objectives primarily through ISE constituent use of the following three pillars, 1) the *ISE Architecture Framework Alignment*, 2) the *ISE Standards and Specifications Framework*, and 3) the *ISE Common Templates* (which guide development of common interoperability artifacts).

Transparent, accountable and properly managed, with full awareness of technical, legal, and civil rights issues, the finished ISE I^{2}F should be made available as widely as possible amongst relevant agencies; namely defense, foreign affairs, homeland security, intelligence, law enforcement, the private sector and industry.

[6] http://serviceorientation.com/serviceorientation/service_orientation_and_interoperability

APPLICABLE POLICIES AND DIRECTIVES

To have optimal effectiveness the ISE I^2F Framework must seek interoperability of all relevant systems and must be supported by stakeholders at all levels. To do this there are political/cultural challenges as well as technical ones. There are multiple authorities consolidated in the ISE I^2F that are covered by numerous presidential directives, policy documents, strategies, committees, and agency guidelines notably:

- The Federal IT Shared Services Strategy
- The Digital Government; Building 21st Century Platforms to Better Serve the American People
- The Common Approach to Federal Enterprise Architecture
- The National Strategy for Information Sharing and Safeguarding
- A Credential Reliability and Revocation Model for Federated Identities
- Executive Order for Responsible information Sharing
- Executive Order – Making Open and Machine Readable the New Default for Government Information

ISE I^2F USAGE

The ISE I^2F is a framework from which concrete reference architectures and implementations are used to share or exchange information. Because the ISE I^2F is based on well-known existing architecture and information management practices (e.g., project management, requirements analysis, architecture development), the ISE I^2F is used to align current disciplines of and methodologies (i.e., service-oriented architectures (SOAs)[7] and codified architecture frameworks) for designing service while retaining consistency with the foundational principles of the ISE I^2F.[8]

The stakeholder's role, relevancy and recommended use of the ISE I^2F by its stakeholders is delineated in

[7] http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51207
[8] http://www.whitehouse.gov/omb/e-gov/fea , OMB CRM DRM.

Table 1.

Table 1. Core Participants

STAKEHOLDER	ISE I^2F APPLICABILITY	HOW TO USE THIS DOCUMENT	RELEVANT ISE I^2F SECTION(S)
Executives – With a responsibility to champion the benefits of the system interoperability and information sharing	• Provides context regarding the scope and relevancy of interoperability to achieve responsible information sharing in support of national priorities • Endorses the use of standards and frameworks in agency level policy • Ties to operational domains and emphasizes "value propositions"	• **Adopt** ISE I^2F (IL) to align National Priorities of Information Sharing and Safeguarding to mission/business objectives and capability • **Adopt** interoperability and capability defined for policy use • **Prioritize** information sharing and safeguarding investments	• Executive Summary • CH 1: Introduction • CH2: ISE I^2F Integrated Landscape • CH 8: Way Forward
Program Managers, Business Owners – Required to challenge the functional requirements and definitions, program development and alignment to mission need and capability	• Describes frameworks and management practices that can deliver agnostic capability • Includes use cases and scenarios applying ISE I^2F concepts • Documents interoperability requirements, reference architecture templates, etc.	• **Implement and measure** ISE I^2F IL through clear goals and benefits of interoperability to be achieved • **Extend** agency roadmap for shared, managed services; identity and access management; data aggregation; cloud; mobile; etc. • **Extend and implement** business and operational capability through use cases and scenarios provided (SARs, RFIs, maritime)	• CH 2: ISE I^2F Integrated Landscape • CH 3: ISE Interoperability Framework • CH 4: ISE I^2F Alignment to Architecture Frameworks • CH 5: Building Interoperability into Mission-Based Architectures • Appn B: ISE Architecture Framework Alignment Grid
Solution Architects, Enterprise Architects, Developers – Required to monitor, challenge, and implement specific technical issues of interoperability, architecture, and others	• Provides specificity regarding standards and services to enable interoperability • Elaborates on interoperability requirements in specific business segment through reference architectures • Includes templates to document interoperability requirements, reference architectures, etc.	• Use ISE I^2F IL to **integrate common architecture** into as new or existing methods • **Use** interoperability standards and specifications • **Extend** capabilities through interoperability reference architecture template method	• CH 4: ISE I^2F Alignment to Architecture Frameworks • CH 5: Building Interoperability into Mission-Based Architectures • Appn B: Architecture Framework Alignment Grid • Appn C: Interoperability Maturity Model • Appn D: ISE I^2F Reference Architecture Template

In the context, mission scope, and authorities of the ISE, the ISE I^2F provides a pathway to align the strategic goals and objectives of departments and agencies with regard to the ISE. The intent of the ISE I^2F is to facilitate interoperability and information sharing. The ISE I^2F builds upon and leverages existing policies, business practices, and technologies in use by Federal and SLTT governments in a manner that fully protects the legal rights of all United States persons.

The relevancy and how to use the ISE I^2F and additional participants are elaborated in Table 2.

Table 2. Additional Participants

STAKEHOLDER	ISE I^{2}F RELEVANCY	HOW TO USE THE ISE I^{2}F
Federal Partners (OMB, GAO) – required to demonstrate alignment to Federal performance, guidance, drivers, and methods as repeatable approaches and governance	• Demonstrates alignment to Federal guidance, drivers, and approaches • Provides an approach that allows for easier performance measurement and improves information sharing and interoperability maturity of ISE stakeholders	• **Adopt** ISE I^{2}F IL and Reference Architecture Template • Aligns National Strategies and Guidance into an integrated view to achieve maturity through business and technical disciplines and best practices • Provides Reference Architecture Template and Architecture Framework Alignment Grid to streamline development efforts
SLTT	• Shows interoperability concepts, standards and services approaches being utilized by Federal partners within the ISE to better align architectures, systems, applications, and capabilities	• **Reuse** cross-cutting subject matter expertise through domain-specific requirements • Streamlined and vetted concepts • Exchange patterns and documentation • Standards and specifications
Private Sector – Businesses and commercial entities that endeavor to work towards building normative standards and services and use them in relevant products	• Shares the standards and services approaches being mandated/ recommended within the ISE to better align vendor products	• **Implement** business and technical capability defined for interoperability and information sharing needs • Support for acquisition processes • Participate as member of standards development organizations
Foreign/International Partners – Asked to examine and implement universal system and interoperability concepts appropriate to them	• Focuses on universal concepts (non-government unique, voluntary consensus standards) • Aligns to in-progress efforts such as the Unified Architecture Framework	• **Adopt** ISE I^{2}F IL management practices • Accepted and tested standards and specifications to meet interoperability objectives

Success of the ISE I^{2}F depends on the degree of cooperation, coordination, and alignment among ISE participants. Further, the ISE must align with, complement, and support the individual missions of the ISE participants. This framework is a flexible and standards-based approach to enable information sharing and reuse across the federal government via the standard description and discovery of common data and the promotion of uniform data management practices.[9]

NOTE: The following are designed to help create the necessary products and artifacts to both assess the current state of a mission architecture's interoperability and help lead to enhanced interoperability.

- Chapter 5 (Building Interoperability into Mission-Based Architectures) provides a 'how-to' overview of each of the sub-processes in the appendices B, C, and D.

[9] http://www.whitehouse.gov/omb/e-gov/fea, OMB CRM DRM.

- Appendix B (Architecture Framework Alignment Grid), ("the alignment grid") details alignment of the ISE I^{2}F to reference architecture frameworks to achieve operational capabilities.
- Appendix C (Interoperability Maturity Model), to validate the processes that are currently employed to exchange information. and
- Appendix D (ISE I^{2}F Reference Architecture Template), to provide a mission agnostic approach to building mission specific reference architectures that will result in an enhanced interoperable reference architecture which is specific to a mission when context is applied.

CONTINUOUS IMPROVEMENT

Interoperability is a highly complex and ambitious proposal—but it offers enormous long-term benefits for reusable "modular" approaches to exchanging data among partners, and will enable such modular approaches to be easier to execute, more efficient to reuse, and less expensive to produce.

Implementation of information interoperability will be in stages. Certain domains, such as security and data structures, will have precedence over others. To start with levels of interoperability in some areas may be limited as individual agencies move to fully adopt the ISE I^{2}F. Over time, the levels of interoperability will steadily improve services to analysts as they use the resources of the ISE to monitor and predict threats.

The ISE I^{2}F welcomes feedback, additional thoughts, and open dialog on the idea of advancing whole-of-government information sharing environment.

1 INTRODUCTION

1.1 VISION AND SUSTAINABILITY

This *ISE* I^2F [10] will drive long-term information sharing requirements by encouraging reuse of capabilities for improvement and information systems planning, investing, and integration to support the effective conduct of U.S. counterterrorism activities. The ISE I^2F will also support shared services development to deliver operational capability through the use of Architecture, Standards, and Profile development and discovery, implemented as a repeatable service methodology.

Discover existing capability or managed services

Build new capability

Extend/reuse existing capability

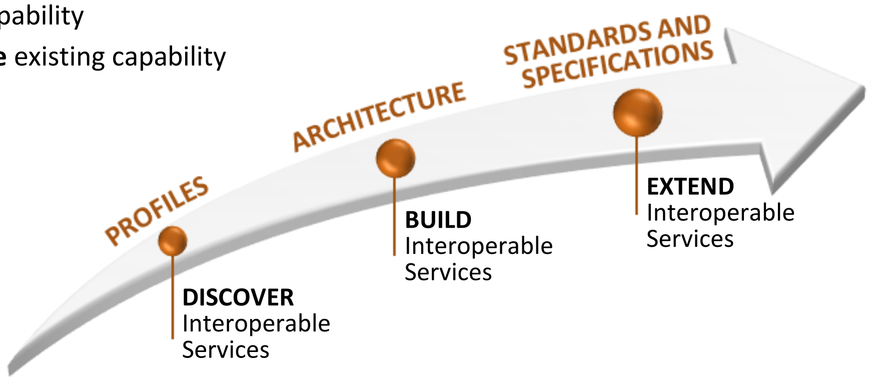

STANDARDS AND SPECIFICATIONS
ARCHITECTURE
PROFILES
EXTEND Interoperable Services
BUILD Interoperable Services
DISCOVER Interoperable Services

Figure 1. ISE I^2F Repeatable Integrated Continuum

1.2 SCOPE

The ISE identifies a set of desired capabilities and leverages existing systems, processes, policies, and information. The ISE enables the sharing of information within three security domains: 1) Unclassified/Controlled Unclassified Information (CUI)/Sensitive but Unclassified (SBU), 2) Secret/Collateral, and 3) Top Secret (TS)/Sensitive Compartmented Information (SCI).

IRTPA 2004 further requires a description addressing the impacts of the ISE on enterprise architectures of participating agencies.[11] Similarly, the *December 2005 Presidential Memorandum* directs building the ISE upon existing Federal Government resources that include standards,

[10] The Office of Management and Budget (OMB) has suggested the term “interoperability framework” for the ISE rather than “enterprise architecture” to highlight the fact that the ISE is a cross-agency construct to be used as guidance for agencies developing the information sharing aspects of their enterprise architectures. The term “enterprise architecture” is used in the OMB context to refer to the architectures prepared by Chief Information Officers to manage the information technology resources of a specific department or agency.

[11] 6 U.S.C. § 485(e)(2).

systems, and architectures,[12] as shown in the Federal Enterprise Architecture v2 levels of scope in Figure 2.

ARCHITECTURE LEVEL	SCOPE	MISSION IMPACT	PLANNING DETAIL	AUDIENCE
International	U.S. and Other Governments	Global Outcomes	Low	All Stakeholders
National	U.S.-wide	National Outcomes		
Federal	Executive Branch	Government Outcomes		
Sector	Multiple Agencies	Mission Outcomes	Medium	Business Owners
Agency	One Agency Organization	Mission Outcomes		
Segment	One or More Business Units	Business Outcomes		
System	One or More Systems	Functionality	High	Users and Developers
Application	One or More Applications	Functionality		

Figure 2. FEA Levels of Scope

1.3 GOALS AND BENEFITS OF INTEROPERABILITY

Investing in interoperability is a strategic investment in a national asset.[13] A shared understanding of information needs, business drivers, legal and policy constraints, interoperability funding requirements, and clear lines of responsibility and accountability will act as significant enablers for responsible and accountable information sharing. Full interoperability should enable the execution of cross-agency processes that can deliver seamless services to ISE participants to counter terrorism in the service of our citizens, guarantee that different systems involved in such processes share information in a semantically-compatible manner, and support the widest possible access to information and capabilities available in the government environment.[14] The benefits of interoperability include:

- Increased information sharing;

[12] Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment (White House: Washington, DC, 2005), Section 1, found at http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html.

[13] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf

[14] Semantic Interoperability Architecture for Electronic Government.

- Integrated planning and enhanced government service delivery;[15]
- Reduced costs of information collection and management;[16]
- Improved decision making;[17]
- Improved the timeliness, consistency, and quality of government responses;[18]
- Improved accountability and transparency of information for citizens;[19]
- Reusable, collaborative methods;[20]
- Improved security;[21] and
- Improved readiness of partners to exchange and share information.[22]

1.4 ISE PARTICIPANTS

Unless otherwise specified in this document, the term "ISE participants" means all federal, state, local, tribal, and territorial (FSLTT) entities, private sector organizations, and foreign partners that participate in the ISE. The ISE serves five communities:

- Defense
- Foreign Affairs
- Homeland Security
- Intelligence
- Law Enforcement

Within each of these entities are first responders, operators, analysts, decision makers, and investigators who have information to share and need information to accomplish their missions. It is the goal of the ISE to provide the ways and means to make terrorism information available, discoverable, and useful by all ISE participants.

[15] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf
[16] http://www.whitehouse.gov/omb/circulars_a130_a130trans4#4
[17] http://www.whitehouse.gov/omb/circulars_a130_a130trans4#4
[18] IRTPA Section 1016.
[19] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf
[20] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf
[21] http://www.ise.gov/sites/default/files/EOResponsibleInformationSharing.pdf
[22] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

This page intentionally left blank.

2 ISE I2F INTEGRATED LANDSCAPE

The ISE I^{2}F delivers a management framework for *extensible*, *measurable,* and *implementable* interoperability requirements throughout the lifecycle of an investment. The I^{2}F aligns to the ISE Management Plan[23] and to a set of business-driven approaches that promote interoperability across multiple communities of interest to effectively manage the implementation of strategic priorities for responsible information sharing. The ISE I^{2}F prescribes how enterprise architecture, standard development and profile descriptions can be best utilized to update, adopt, or create reference architecture; it supports systems development efforts and governance principles. This is accomplished through the use of design patterns for information exchange (hereafter referred to as exchange patterns), thus promoting and adopting more efficient service oriented design principles (i.e., loose service coupling, service abstraction, service reusability, and service discoverability) described with additional details in Section 3.3, Technical Capabilities.

Overall, the ISE I^{2}F links three business and technical management disciplines that assist ISE participants meet interoperability requirements within their own operational capabilities. Below is the ISE I^{2}F Integrated Landscape (IL), fulfilled through the **Architecture Framework Alignment**, the **ISE Industry Standards and Specifications Framework,** and **ISE Common Profile.** Figure 3 is a diagram of these integrated disciplines.

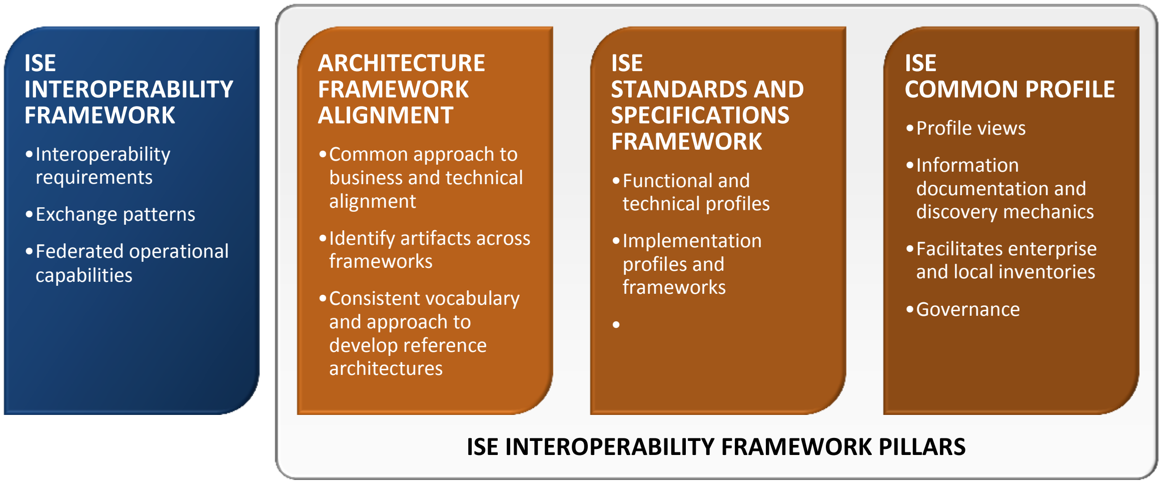

ISE INTEROPERABILITY FRAMEWORK
•Interoperability requirements
•Exchange patterns
•Federated operational capabilities
ARCHITECTURE FRAMEWORK ALIGNMENT
•Common approach to business and technical alignment
•Identify artifacts across frameworks
•Consistent vocabulary and approach to develop reference architectures
ISE STANDARDS AND SPECIFICATIONS FRAMEWORK
•Functional and technical profiles
•Implementation profiles and frameworks
•
ISE COMMON PROFILE
•Profile views
•Information documentation and discovery mechanics
•Facilitates enterprise and local inventories
•Governance
ISE INTEROPERABILITY FRAMEWORK PILLARS

Figure 3. ISE I^{2}F Framework Integrated Landscape

Over the long-term, the ISE I^{2}F will facilitate development of a confidence and trust-based culture in interoperability; communities will look to discover existing standards and capabilities (e.g., managed services) before they focus on developing their own.

[23] ISE Management Plan

Success for ISE I^{2}F adoption can be defined as a state in which agencies and mission partners:

- Attempt to explore and discover existing interoperability capabilities and standards that either meet their requirements, or can be easily extended to develop new capabilities;
- Follow a governance structure that helps uniformly define a common profile for these capabilities so that they can be consistently tagged at source with discoverability metadata based on a common pre-harmonized taxonomy; and
- Contribute to a common and federated repository where these capabilities can be easily discovered for others to reuse.

The following sub-sections (2.1 – 2.4) contain a brief overview of the various components of the ISE Interoperability Framework.

2.1 ISE INFORMATION INTEROPERABILITY FRAMEWORK (I^{2}F)

The ISE I^{2}F provides detailed descriptions of architecture exchange patterns that describe typical information exchange options (e.g., broadcast messages (alerts and notifications) and requests for information (also known as queries)). These exchange patterns provide a high-level description of complex business problems using information models and diagrams. The exchange patterns themselves become the technical solutions to solve the identified complex business problems. Further, the exchange patterns can depict more complex exchange scenarios such as federated or shared message coordination. Each pattern is described and outlined for direct applicability in architecting information exchanges and interoperability requirements. Definitions for federation and federated identities[24] are provided in the context of exchange requirements and organizational needs as aligned to the ISE I^{2}F IL. See Section 3.

2.2 ISE ARCHITECTURE FRAMEWORK ALIGNMENT

The ISE Architecture Framework Alignment is centered upon the ISE Architecture Framework Grid, the first integrated pillar in the ISE I^{2}F. The ISE Architecture Grid provides alignment to several commonly used Architecture Frameworks (listed below), and is baselined specifically to the Federal Enterprise Architecture[25] (Common Approach) domains as a best practice. The grid maps these common architecture domains to requirements and specific artifacts as a consistent and repeatable method.[26] Further, using the Common Approach enterprise architecture domains, the ISE I^{2}F derives the requirements to enable interoperability. Each architecture domain provides the initial alignment criteria and relationships to the ISE I^{2}F, which demonstrates how interoperability

[24] http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7817.pdf

[25] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf

[26] The Common Approach was used as a building block in the development of the Federal Enterprise Architecture Framework (FEAF), Version 2, which is one of the frameworks aligned to in this document.

can be achieved using an architecture framework methodology and implemented within a reference architecture template to support a specific mission capability. See Section 4.

The architecture frameworks aligned to show interoperability include:

- Federal Enterprise Architecture Framework (FEAF), Version 2,[27]
- Department of Defense Architecture Framework (DoDAF),[28]
- The Open Group Architecture Framework (TOGAF),[29]
- Global Reference Architecture (GRA),[30] and
- Intelligence Community (IC) Program Architecture Guide (PAG).[31]

2.3 ISE STANDARDS AND SPECIFICATIONS FRAMEWORK

The ISE Standards and Specifications Framework is the second pillar in the ISE I^{2}F. It provides the descriptive mechanics to develop components, and processes necessary to identify and normalize standards to achieve interoperability. The ISE Standards Specifications framework describes interoperable information exchange attributes beginning with standardized requirements and definitions. This corresponds to the ISE I^{2}F's Operational Capabilities component as described in Section 3. As multiple mission partners recognize their needs, similar capabilities can evolve into common practices that can then be standardized and reused to meet a host of mission needs. Recognizing that specific processes and requirements vary across jurisdictional boundaries, the ISE I^{2}F supports the need to standardize information sharing exchanges into patterns that enable interoperability. The standardization of these exchanges into patterns supports extensibility across unique jurisdictions. Creating standards for interoperability needs supports flexible and robust enterprises. For example, common components of the standards and specifications framework include the development of business and functional requirements along with specific technical requirements for identity and access control (role-based), policy, privacy, conformance, and compliance.

2.4 ISE COMMON PROFILE

The ISE Common Profile is the third pillar of the ISE I^{2}F. The ISE Common Profile describes an implementable construct based on the International Organization for Standardization (ISO)/International Electro technical Commission (IEC) Technical Recommendation 10000-1.[32] The Common Profile characterizes the detailed information for a modular component within an

[27] http://www.whitehouse.gov/omb/e-gov/fea

[28] http://69.89.31.228/~mkerncom/wp-content/uploads/2013/02/Federal-Enterprise-Architecture-Framework-v2-as-of-Jan-29-2013.pdf

[29] http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html

[30] http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015

[31] https://intellipedia.intelink.gov/wiki/Intelligence_Community_Program_Architecture_Guide

[32] http://www.iso.org/iso/home.htm

enterprise so that options, parameters, and other valued choices are appropriately specified to enable interoperability. In the context of the ISE I^{2}F, the Common Profile aggregates and provides references to other supporting information needed to understand a component's fit, form, function, context, and general characteristics for interoperability. The ISE Common Profile is currently under development. A description of the ISE Common Profile is included in section 6. Information Sharing Environment Product Set(s)

The ISE I^{2}F provides authoritative guidance for interoperable information sharing with the approach that establishes a common way to reference applicable standards and specifications and supersedes the following documents as outlined on the ISE webpage:

- The ISE Enterprise Architecture Framework, Version 2[33]
- Profiles and Architecture Implementation Strategy, Version 2[34]
- Common Terrorism Information Sharing Standards, Version 1[35]

Coordination with ISE Management, and Performance Reporting and Planning are accomplished via:

- ISE Management Plan[36]
- ISE Performance Management Framework and Scenario Guide[37]

As the ISE interoperability concepts mature, they will be instantiated in PM-ISE member architectures and future interoperability reference architectures including geospatial, identity and access management, and data aggregation.

[33] http://ise.gov/sites/default/files/ISE-EAF_v2.0_20081021_0.pdf
[34] http://ise.gov/sites/default/files/ISE-PAIS_V2.0_0.pdf
[35] http://ise.gov/sites/default/files/CTISSprogramManual20071031.pdf
[36] ISE Implementation Plan
[37] http://www.ise.gov/ise-performance-management#performance-scenarios

3 ISE INFORMATION INTEROPERABILITY FRAMEWORK (I^2F)

The ISE I^2F describes the components that enable information sharing and interoperability within a given reference implementation. The components of the ISE I^2F framework allow for practitioners to organize information that defines the scope of what needs to be considered to achieve interoperability between ISE participants. Through the use of this information, ISE participants are able to identify touch points for sharing and safeguarding information in motion; while encouraging the use of interoperability within the scope of enterprise architecture concepts that are, and driven by, an organization's internal enterprise architecture framework.

The ISE's participants have recognized the need for integrated and interoperable solutions as a priority. Whereas the solution lifecycle once originated as an independent or a standalone agency requirement, it must now be developed with the enterprise view in mind. The components of the ISE I^2F acts as building blocks to advance the enterprise view for sharing, standardization, and integration across ISE participants. Figure 4 highlights the key components of the ISE I^2F, which are elaborated upon in the subsequent sections.

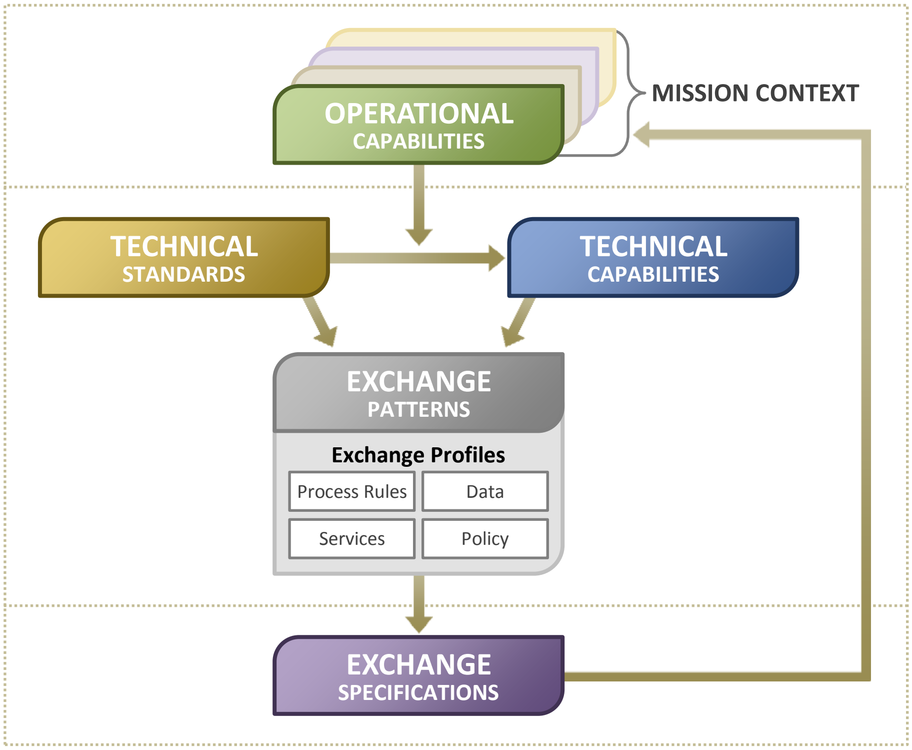


Figure 4. ISE I^2F Components

The components of the ISE I^2F promote mission driven capabilities at the operational layer while de-coupling the technical layer to focus on standardization and interoperability across the ISE's participants.

The ISE I^2F is expected to be implemented within an organizational context to provide guidance for implementation and on-going information and data management strategies. Figure 4 highlights the key components of the ISE I^2F, which are elaborated in subsequent sections.

3.1 OPERATIONAL CAPABILITIES

ISE I^2F *Operational Capabilities* are the reference implementations of standards and services coupled with the appropriate policy, process, training, outreach, and other infrastructure components. As depicted in Figure 4, Operational Capabilities provide the Mission Context or the Mission Need that drives other components of the ISE I^2F. The alignment to the Mission Need is critical to ensure the operational and technical investments for interoperability also enable mission requirements. To support the mission need, *Operational Capabilities* may contain elements that include, but are not limited to, operational policy, requirement definitions, use cases, business cases, implementation guidance, sustenance strategies, and any inter-/intra-agency memorandums of understanding (MOUs). These elements combined validate the need for technical capabilities and standards to exist and interoperate across the ISE, at the same time, providing top-down and bottom-up traceability.

Operational Capabilities; however, do no dictate how a capability is to be achieved at the technical level. This ensures maximum design freedom for the operational and acquisition teams as well as flexibility for the technical team to drive interoperability through approved Technical Capabilities and supporting Technical Standards—explained in the next sections.

3.2 TECHNICAL CAPABILITIES

ISE I^2F *Technical Capabilities* constitute detailed technical descriptions that provide a conceptual view into the technical implementation and the role of technology. Technical Capabilities, also referred to as Technical Services, are divided into categories of like functionality based on the needs of the organization and updated as the needs change. Technical Capabilities, such as 'Structured Data Management Services' are mainly abstract in nature but their impact is in exposing if two Technical Capabilities are interoperable through the use of Technical Standards and Specifications (detailed in the next section). Technical Capabilities: 1) address and support operational needs and requirements, 2) provide reference implementations of one or more technical standards and specifications, and 3) lead to the required technical functionality to realize Operational Capabilities. The goal of ISE I^2F is to encourage interoperability of Technical Capabilities not only internal but across organizations. This allows the ISE participants to:

- Identify new capabilities or re-use existing ones to minimize capability gaps;
- Promote interface standardization across technical capabilities to maximize interoperability and reduce maintenance and operation activities; and
- Recognize and embrace new technology paradigms by assessing maturity and establishing roadmaps for Technical Capabilities.

As described, the most common types of services and Technical Capabilities applicable to information interoperability include, but are not limited to: discovery, messaging, mediation, security, audit (monitoring), collaboration, enterprise service management, and storage. As stated above, *Technical Capabilities* may be referred to as *Technical Services*[38] and can be implemented within an organization or implemented as a *shared service*[39] across multiple organizations.

The *Technical Capabilities* described often are mission agnostic as they are modular building blocks that can be linked internally or externally to other Technical Capabilities to enable sharing and interoperability. This practice is important to the interoperability and the exchange pattern discussion and recommends that services should be developed with fundamental characteristics for *discovery*, *building, or extending* services for citizens, specific groups of citizens, organizations, or multiple organizations. However, based on an organization's maturity, some of these services may be specialized for specific applications or generalized for a larger service area to promote reuse and interoperability. Table 3 below provides a list of Technical Capabilities and Technical Services along with their descriptions.

Table 3. Technical Capability/Service Chart

TECHNICAL CAPABILITY/ SERVICE AREA	DESCRIPTION
Discovery	*Metadata, person, service, and content discovery.* ISE I^{2}F recognizes that the ISE mission partners have different mission applications and needs, and store information about standards, persons, and services differently. However, there is a need for a common taxonomy that helps mission partners find these capabilities consistently.
Messaging	Notifications, alerts, and enterprise messaging.
Mediations	Protocol adaptation and data transformation.
Security	Policy decision (SAML), retrieval (XACML), administration, certificate validation, principle attribute services, and public key infrastructure (PKI).
Audit	Robust auditing capabilities to support accountability, provide discrete non-repudiation, and enhance transparency in security effectiveness.
Collaboration	Conferencing, person discovery, voice over internet protocol (VOIP), collaborative workspaces, and broadcasting.

[38] See Appendix G, Glossary.

[39] https://cio.gov/wp-content/uploads/downloads/2013/04/CIOC-Federal-Shared-Services-Implementation-Guide.pdf

TECHNICAL CAPABILITY/ SERVICE AREA	DESCRIPTION
Enterprise Service Management	Monitoring and quality of service (QoS) of critical resources, service-level agreement (SLA) compliance, exception detection and handling, service utilization, and distributed service management.
Storage	Data source integration and enterprise content delivery network.

3.3 TECHNICAL STANDARDS

ISE I^{2}F *Technical Standards* are intrinsic elements of operational and technical capabilities that are utilized for defining information exchange patterns and information exchange specifications. Technical Standards enable interoperability through advancing design and implementation, so that ISE participants can communicate, exchange data, and make use of the information being shared.[40] The ISE standards are technical and foundational in nature and are either specific to a mission need or expansive to tackle challenges across various communities. Technical Standards relating to a mission are developed in conjunction with practitioners from that mission area. An example of this is the ISE effort to promote standards such as Common Alerting Protocol (CAP)[41] used to disseminate Alerts across the Federal, State, Local, and Private Industry stakeholders. Inversely, Technical Standards relating to capabilities across various communities and organization require general agreement to encourage interoperability rather than fragmentation. An example of these Technical Standards includes the ISE effort to promote Federal Identity, Credential, and Access Management (FICAM) across the Federal Government.

Technical standards are developed by industry organizations, specifically standards development organizations (SDOs), in cooperation with government and industry stakeholders. Technical standards are usually published as a normative standard specification (e.g., National Information Exchange Model[42] (NIEM), Extensible Mark-up Language (XML), or Web Services Specifications (WS*) that is used to define and measure conformance to interoperability. With the help of these tools, ISE participants focus on standards ranging from data, exchange protocols, services, and metadata standards. However, ISE I^{2}F does not attempt to dictate how mission applications or tools implement the agreed upon standards.

Subsequent sections of the document, Section 3.5, describe the relationship between Technical Standards and Exchange Specifications.

[40] Program Manager of the Information Sharing Environment. *Information Sharing Environment Administrative Memoranda (ISE-AM): Common Terrorism Information Sharing Standards (CTISS) Program (2007).* http://ise.gov/sites/default/files/ise-asm300-ctiss-issuance.pdf

[41] http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

[42] National Information Exchange Model (NIEM) Standard

3.4 EXCHANGE PATTERNS

ISE *exchange patterns* provide generic solutions to help demonstrate a commonly occurring need for exchange of data or information. A pattern is a description of a core function within an information sharing transaction, and should be described and cataloged along with interoperability technical standards and services requirements as part of an information exchange specification.

An exchange pattern may be developed by different groups within or between organizations depending on the maturity of the organization(s). While most organizations are becoming proficient at defining information exchanges, interoperability often requires an evolved governance model that requires different groups within the organization to agree on the interoperability requirements. Furthermore, the governance model establishes a standardized way of developing patterns that project teams may implement as they develop their mission-specific applications.

The following sections provide details on components of an exchange pattern, and their relationship(s). The ISE exchange profile is used to document the core components of the ISE exchange patterns for an information sharing transaction is the context of the process rules, data, services, and policy related to the exchange pattern. The ISE exchange specification applies the principles of the context for an exchange into specific technical specifications, standards, and mechanisms necessary to develop interfaces for the exchange. A federation is an organization of interoperating networks or service providers that apply common governance and processes to implement interoperable information sharing that implements ISE exchange profiles, patterns, and specifications.

3.4.1 CONCEPTUAL EXCHANGE MODEL

The ISE I^{2}F *Conceptual Exchange Model* (Figure 5) is a high-level architecture model that aligns three basic information sharing patterns (query/response, broadcast – alerts/warning/notification, and workflow). The Model aligns mechanisms associated with interoperability requirements where more than one exchange pattern is combined to address specific information exchange needs. The orchestration and choreography information exchange hubs are represented in the more complex patterns relating to coordination and messaging broker services.

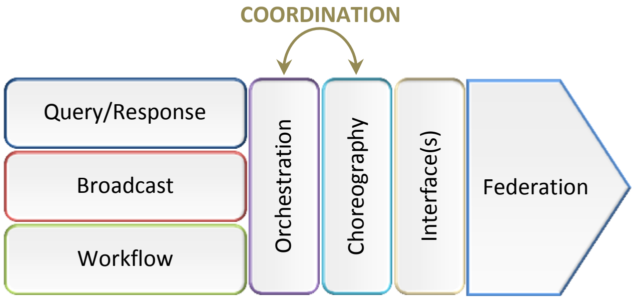


Figure 5. ISE I2F Conceptual Exchange Model

3.4.1.1 STANDARDIZED INTERFACES AND INTEROPERABILITY

In the context of the ISE I^{2}F, Interfaces are protocols or specifications used to transfer information between systems. The concept of interfaces, application program interfaces (APIs), or end points represent the points where technical components of an information exchange interact. This interaction can be within the information flow of a single system, or it can be at a point that serves as a boundary to the system—but any interface is characterized primarily as a point where a handoff of information occurs—regardless of what exchange pattern the handoff reflects. Documenting each of these interfaces with the specific technical information necessary to develop another service to interact with that interface is key to achieving interoperability, and is the purpose of the ISE exchange specification.

The ISE exchange profile, pattern, and specification focus on these points for information handoff because they are the point of maximum return for enhancing information exchange between systems without interfering with the solution architecture that system owners deem most appropriate. As long as the implementation of the information exchange interface, API, or end point is properly documented, the freedom of the system owners and architects is maximized to choose the network or system architecture most appropriate for meeting their mission or business need—whether it be an open source application, proprietary COTS software, data center appliance, or cloud-based utility—so long as that solution is capable of translating its data into the structure required by the interface documented in the ISE exchange specification. The use and clear documentation of established standards and protocols enables whatever solution architecture is chosen to achieve interoperability with diverse other solution architectures and systems.

The ISE exchange profile will document the business-level aspects of the interface for the exchange pattern allowing for a reference architecture or technical guidance view into the interface, sufficient to allow executives, program managers, and business owners to understand the function and purpose of the interface as part of the exchange pattern. The exchange specification, on the other hand, will contain the technical implementation details necessary to establish an instance of the interface, or to interact with it, and is described at the level that a solution architect, enterprise architect, or developer would need to understand how the interface should be implemented.

3.4.2 QUERY/RESPONSE PATTERN

The query/response pattern (Figure 6) is the most common type of information exchange transaction. A sharing partner (service consumer) initiates a request, and a second partner (service provider) may respond to that request with either the requested information or call to a specific resource to obtain the information.

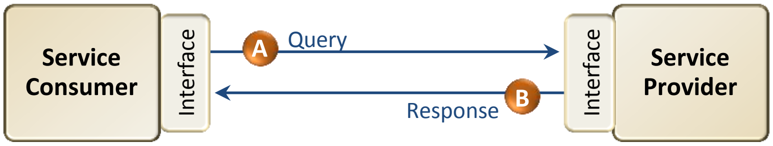


Figure 6. Query/Response Pattern

3.4.3 BROADCAST PATTERN

A broadcast exchange pattern (Figure 7) can be an independent alert, warning, or notification exchange pattern that is disseminated to a varied set of mission partners across multiple mission areas to communicate details of a specific incident or event(s), and even solicit real-time operational assistance with specific event or case related actions.

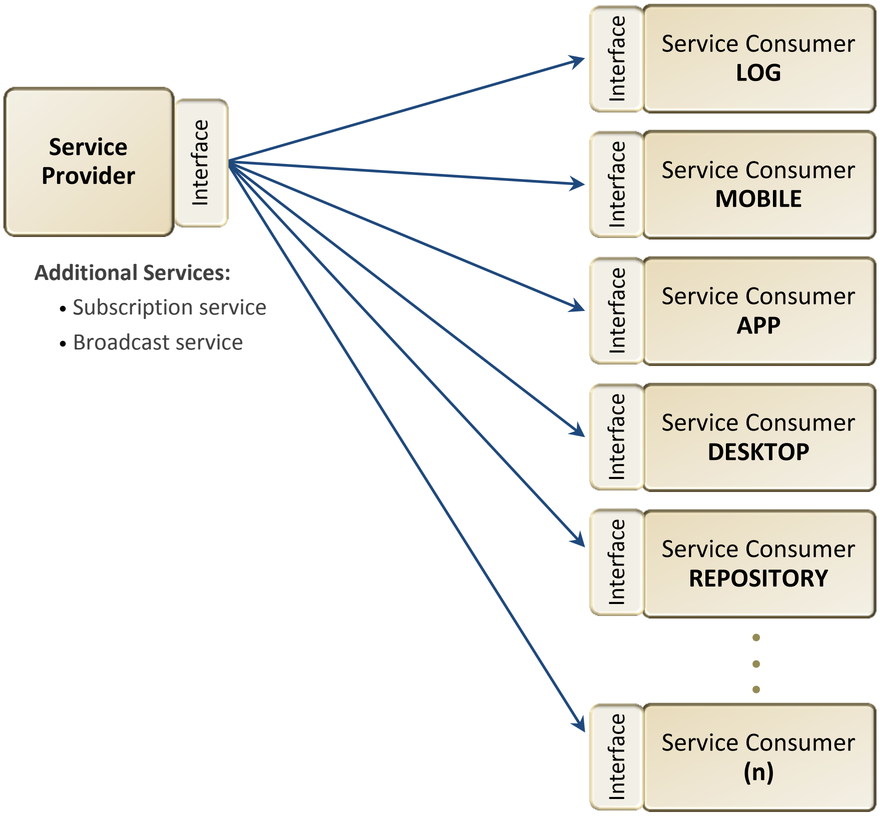


Figure 7. Broadcast Pattern

Exchange patterns for broadcast messages will include similar elements as documented in the query/response pattern. However, these elements will be further elaborated to define implementation options, including architecture context and associated messaging depending on the type of broadcast. These options would include (along with architectural impact) situations where a service provider broadcasts messages to specific service consumers in a point-to-point messaging pattern, or in a publish-and-subscribe construct where the service provider publishes the broadcast message to a subscription service. These subscription services manage downstream technical requirements capabilities like mediation and transformation services, content based routing, etc. In most cases there is a system-level acknowledgement that confirms that the message was delivered successfully, with no real mission-specific responses expected as part of this pattern.

3.4.4 WORKFLOW PATTERN

Workflow pattern (Figure 8) exchanges are typically part of an organization's operational environment where information is routinely moved across mission partners to accomplish day-to-day operational requirements. An example of such an exchange would be a police department sharing complaint information with a court's case management system. This exchange initiates the creation of a case on the court's docket and improves operational efficiencies by minimizing redundant data entry and associated data re-entry errors.

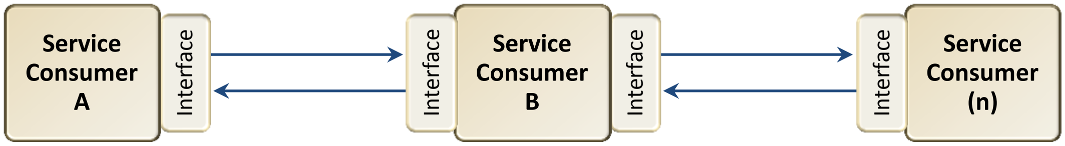


Figure 8. Workflow Pattern

3.4.5 COORDINATION PATTERN(S) – ORCHESTRATION AND CHOREOGRAPHY

Orchestration is accomplished through the widespread deployment of standardized and composable services, each of which encapsulates a segment of the enterprise and expresses it in a consistent manner. Orchestration is the mechanism to define the sequencing interdependencies of multiple services leading to consolidated/enriched response to the endpoint.

Choreography is accomplished by defining how messages should flow among interconnected applications and systems to ensure optimum interoperability. Choreography includes tools for defining how multiple parties collaborate in peer-to-peer, service-oriented business transactions. Choreography can be abstract - exchanged messages defined by data type and transmission sequence; portable - defining the data type, transmission sequence, structure, control methods, and technical parameters; or concrete - similar to portable choreography, but including the source and destination (e.g., URLs) as well as security information.

Orchestration shows the complete behavior of each service whereas the choreography combines the interface behavior of each service.

Different options may include scenarios where:

- An initial request leads to a number of similar or related responses from multiple sources (Figure 9). A request may trigger the query of similar information from multiple sources, and the responses are consolidated, i.e., orchestrated, to provide a uniform view (if semantically possible) for the service consumer.

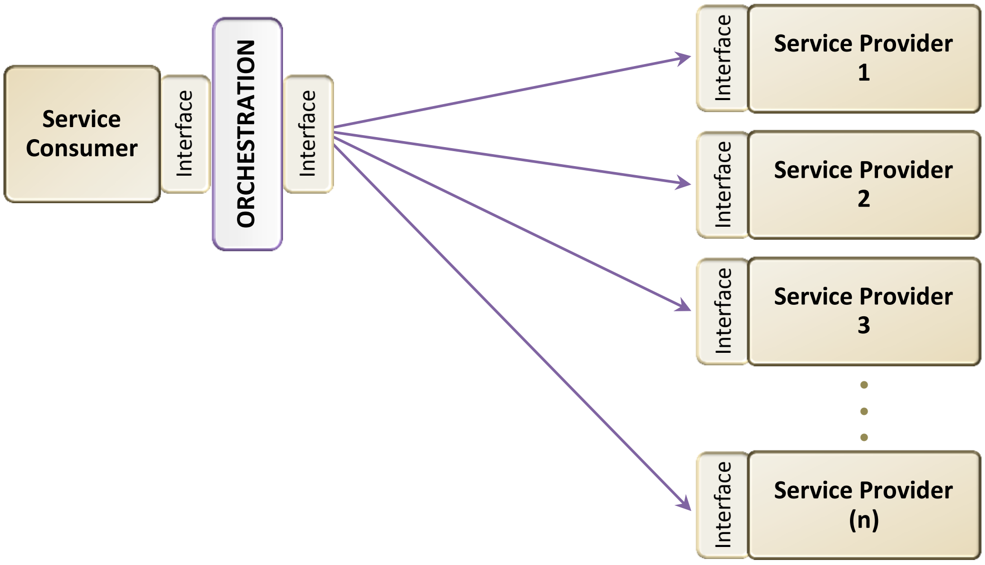


Figure 9. Coordination Pattern – Orchestration

- An initial request (Figure 9) leads to a number of similar or related responses, often with enriched data. The request is based on a predefined sequence of services), where a response from one query provides input parameters for subsequent services. Figure 10 depicts the choreography pattern, the coordination of these query responses into input parameters as they flow through subsequent services. The choreography of these services might generate alerts and warnings based on specific data inputs, events, or thresholds. These exchanges are fairly complex and incorporate a number of different types of technical patterns and capabilities.

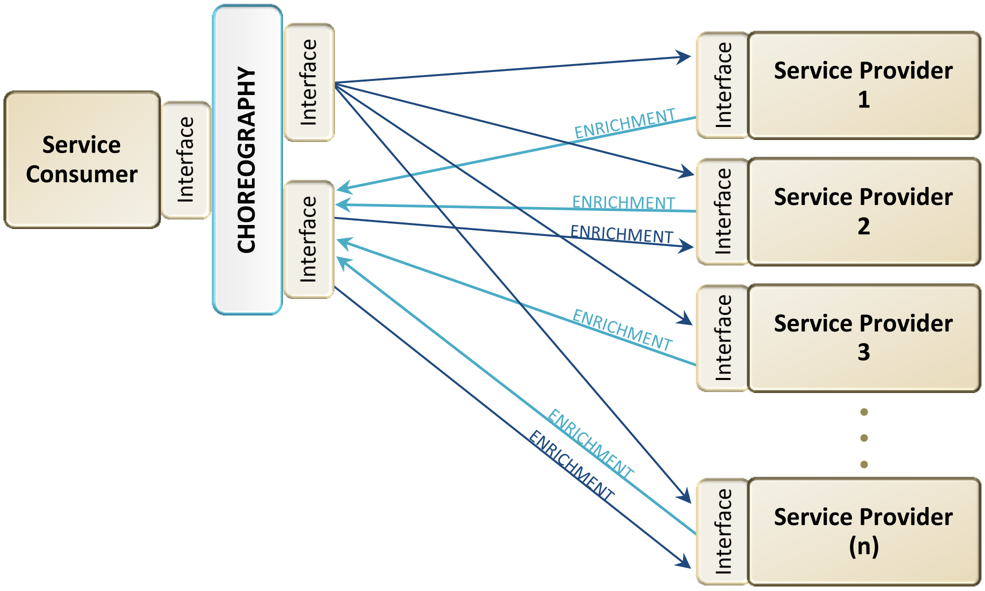


Figure 10. Coordination Pattern – Choreography

3.4.6 EXCHANGE PROFILE(S): ELEMENTS AND ATTRIBUTES

The standards relevant to information sharing and interoperability requirements, as abstracted in the exchange patterns are categorized as part of an ISE **Exchange Profile**, consisting of, but not limited to, the following elements: Process Rules, Data, Services, and Policy. These elements align to the attributes necessary for interoperable services between one or more information systems.

3.4.6.1 PROCESS RULES: CONTEXT AND USE

Process rules represent the purpose and scope of the sharing content. Process rules are defined as the rules associated with the exchange profile that allow the exchange package, such as an Information/Exchange Package (IEP) in the form of a XML schema, to play a role in a workflow or a complex multi-exchange environment. Process rules in a workflow might require a digital signature, provide output via reports, notifications etc., or support multiple events (business rules) in a given workflow. The process rules section of the ISE exchange profile may include the following attributes:

- High level description and purpose of the exchange
- Key stakeholders and participants, and their roles
- Exchange definitions in a broader business capability
- Normalized information of the exchange content
- Mechanisms to reuse and extend the exchange as needed to meet specific mission applications without compromising the semantic meaning of the content or the interoperability requirements
- Description of rules and enforced implementation guidance, if available
- Description of any shared services that might be used in processing the exchange

3.4.6.2 DATA: CONTEXT AND USE

Data represents the mission information that needs to be shared and how it is represented. Data (or information) interoperability is initiated as the exchange partners agree on a common (and accurate) vocabulary that represents the business needs and preserves the semantic meaning of the information being exchanged. An example of a common vocabulary is the National Information Exchange Model (NIEM).[43]

Data interoperability is achieved when the exchange partners or the community agrees upon an information exchange package to reflect their specific mission needs. These include standards for vocabularies, ontologies, and models that represent the information that enables clear and unambiguous communications between infrastructure domains, irrespective of the technology

[43] https://www.niem.gov/Pages/default.aspx

products and/or solutions used. The content is produced and consumed without losing the intended semantics and meaning of the exchanged message. Data standards are applicable to a wide range of elements to include raw collected data, messages, and published documents and records. An example of a data standard is the Geographic Markup Language (GML).[44]

Data is a significant component of the pattern; the specific data elements are mission and exchange requirement specific, and best described in the ISE exchange specification section. The data section of an ISE exchange profile, in contrast to the ISE exchange specification, may include the following attributes:

- Description of the type or categories of data to be included in the pattern
- Recommendations/suggestions for specific data standards that may be used
- Methodology and standardized[45] tags for metadata tagging of the payload, and fine grain tagging for specific data elements to indicate identity and access management, security classifications, privacy and civil liberties, use and dissemination, provenance, etc. (if available and applicable)
- As federal systems implement compliance with EO 13587 and NSISS requirements for automated, policy-based access control, the data section should additionally include descriptions of sources of automated access control rules that apply to the data, including a link to the authorities for those rules listed in the exchange profile policy section that are intended to be enforced in access controls for the data.

3.4.6.3 SERVICES: CONTEXT AND USE

Services represent how mission information is shared, and provide the mechanism that specifies the technical protocols, and communication headers, parameters and attributes, etc. At this level, services may be abstracted to reflect components that need to be addressed consistently for information sharing. These components would include information about service endpoints, connection protocols, and metadata/taxonomy that enables service discovery, and mediation. However, within the mission, and the architectural context, services may be implemented in a number of diverse technology constructs like Web Services, Restful Services, Message Queues (MQ), etc. Attributes of the services section of the ISE exchange profile may include:

- Type of service
- Number of endpoints

[44] http://www.opengeospatial.org/standards/gml

[45] For the purposes of this document, “standardized” tagging refers to data taxonomies and metadata schemes developed to reflect policy rules relating to data (typically controlled data) on federal information systems. Such standardized data tagging would include that in line with functional requirements and technical specifications being developed under the auspices of the IISC for Priority Objective #3 of the National Strategy for Information Sharing and Safeguarding, or similar efforts at IC or DoD for classified networks. Tagging done within a system or application that is internally consistent to that system or agency but not standardized to metadata tagging standards developed in such larger, interdepartmental efforts, is unlikely to be sufficient to meet interoperability requirements that support access control, discovery, correlation, or records management, and should be disfavored.

- Description of endpoints
- Connection protocols
- Connection parameters including IP addresses, security/identity assertions, etc.
- Metadata for service discovery (based on standardized taxonomy, if available)
- Methodology and standardized tags for metadata tagging of the service specification to indicate identity and access management, security classifications, privacy and civil liberties, use and dissemination, provenance, etc.

3.4.6.4 POLICY: CONTEXT AND USE

Policy represents the metadata associated with an exchange that describes rules associated with discovery, sharing, security classification, use, and dissemination of data. Policies may be applied to the entire data exchange, or may be more granular where different types of policies are applied to specific data elements or datasets. Typical application of policies includes tagging of data and services for personally identifiable information, application of identity and access control rules, etc. Attributes of the policy section of the exchange profile may include:

- Description of applicable policies;
- Methodology referenced in previous description of data and services; and,
- Rules around how tags may be applied including interdependencies, sequencing, and application of these rules.

3.5 EXCHANGE SPECIFICATIONS

The exchange specification is the instantiation of an exchange pattern, and once implemented correctly enables real interoperability. While the ISE exchange profile provides the structure that enables interoperability and provides key considerations and questions to be asked during implementation(explaining the business considerations for executives, program managers, or business owners) an ISE exchange specification is where developers, solution architects, and enterprise architects go to document or find specific information is provided for the exchange to be implemented, questions are answered, and specific decisions are made to address key considerations.

The exchange specification—an executable, implementable view of an exchange pattern—is based upon specific requirements and supports specific assumptions about the expected deployment architecture or runtime environment. Exchange specifications extend the abstract concepts in the exchange patterns by:

- Applying the business (i.e., mission) requirements, rules, and/or policies for mission-specific use;

- Defining the data structures, tags, and other relevant attributes (policy) of the information to be shared (data); and,
- Specifying the mechanism involved in the exchange of the information (services).

Exchange specifications may be developed in collaboration with mission partners by applying mission context to the technical standards. Once adopted by a community of interest, exchange specifications significantly enable interoperability across agencies and jurisdictions within that community.

An exchange specification may be developed by a project team with a specific need to implement that capability, or may be a joint effort across multiple teams with a common need. This requires a mature governance model to ensure adequate change control management. An exchange specification is (i.e., becomes) the contract between service producers and consumers that is used to develop interfaces. Even a minor change in the specification without appropriate change management may break operational systems and capabilities. In many cases this type of governance is also provided by industry consortia and standards bodies that help develop some of these exchange specifications into national standards available for use by multiple organizations.

See ISE I^2F section 7.4 for additional information on the implementation view of exchange specifications, related to the common profile.

3.6 FEDERATION

A Federation is multiple computing and/or network providers agreeing upon standards of operation in a collective fashion.[46] Federation helps define the rules of engagement, MOUs, common operating processes, and technical standards and specifications that allow all members of the federation to participate and leverage the capabilities offered by the member organizations.

3.6.1 FEDERATED IDENTITIES PATTERN

Federating identities in information technology is the process of linking a person's electronic identity and attributes, which are stored across multiple distinct identity management[47] systems, within a trust framework agreed to by the participants in the federation. The trust framework establishes the ground rules for participants, as elaborated in the federation's agreed-upon governance documents, documented processes, and technical specifications. The federated users are able to access multiple capabilities offered by participants by asserting their trusted identities and specific attributes without the need to provision each user in each of the participant systems.

[46] http://en.wikipedia.org/wiki/Federation_%28information_technology%29
[47] http://en.wikipedia.org/wiki/Identity_management

Federation is enabled through the use of open industry standards and/or openly published specifications, such that multiple parties can achieve interoperability for common use. Typical use involves web-based single sign-on, cross-domain user account provisioning, cross-domain entitlement management, and cross-domain user attribute exchange.

3.6.1.1 IDENTITY EXCHANGE PATTERN

A specific example of a non-generic information exchange pattern is an identity exchange pattern. Identity is a constant for enterprise systems that inevitably involves coordination of at least several query/response exchange patterns, but typically is far more complicated in the enterprise and involves a complex coordination pattern. As identity management for user authentication evolves into more elaborate systems for identity, credentialing, and access management, analyzing identity in the context of exchange patterns helps to highlight the conceptual points in the identity process where an interface could be exposed to: 1) improve the strength of the user's system identity, 2) to apply that strongly authenticated identity to the network security processes (for instance, by providing better user tracking for audit and continuous diagnostics and monitoring), and 3) to provide fine-grained policy-based access control to sensitive resources on the system.[48] As these conceptual points for potential interfaces in an exchange are identified, developers, enterprise architects, and solution architects are enabled to more effectively adapt their system by identifying the interfaces and additional exchange patterns needed to evolve their mission applications, and security processes, as well as locate where in the system those interfaces and patterns need to be applied.

3.6.1.2 FEDERATING IDENTITIES

The federation of identity describes the technologies and standards which serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Identity federation comes in a variety of instantiations, including "user-controlled" or "user-centric" scenarios, as well as enterprise-controlled or business-to-business scenarios.

An advantage of approaching identity as an aggregation of exchange patterns is that the interfaces and patterns identified internal to the system can be leveraged to facilitate participation in identity federations. Developers, enterprise architects, and solution architects can use the exchange patterns identified for their own systems to either take advantage of existing interfaces or to create the new interfaces or exchange pattern instantiations necessary to exchange identity information with other federated systems.

[48] For instance, strong authentication is one of the Federal Cybersecurity Cross-Agency Priority Goals for FY13, and the *National Strategy on Information Sharing and Safeguarding* makes improving identity, credential, and access management one of the top five priority objectives for the federal government.

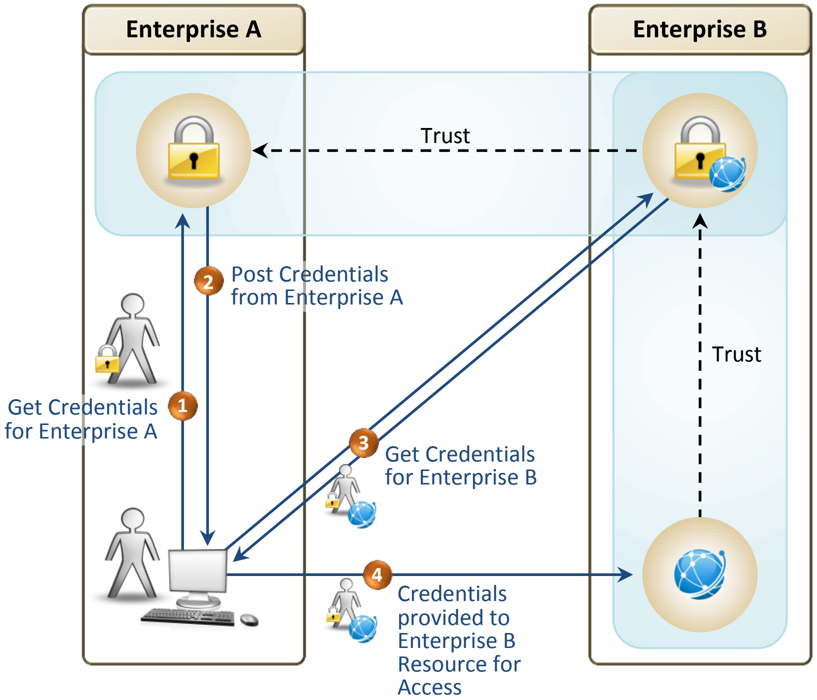

Enterprise A
Enterprise B
Trust
Trust
2 Post Credentials from Enterprise A
1 Get Credentials for Enterprise A
3 Get Credentials for Enterprise B
4 Credentials provided to Enterprise B Resource for Access

Figure 11. Federated Identity Pattern

3.6.2 FEDERATED QUERIES PATTERN

A federated query is an implementation of the orchestration pattern, as explained in Section 3.4.5, where a user is able to access multiple repositories based on a single query. Figure 12 shows a simple federated query pattern. This pattern is one of many published *service oriented architecture patterns* normalized by an international community of architects and practitioners.

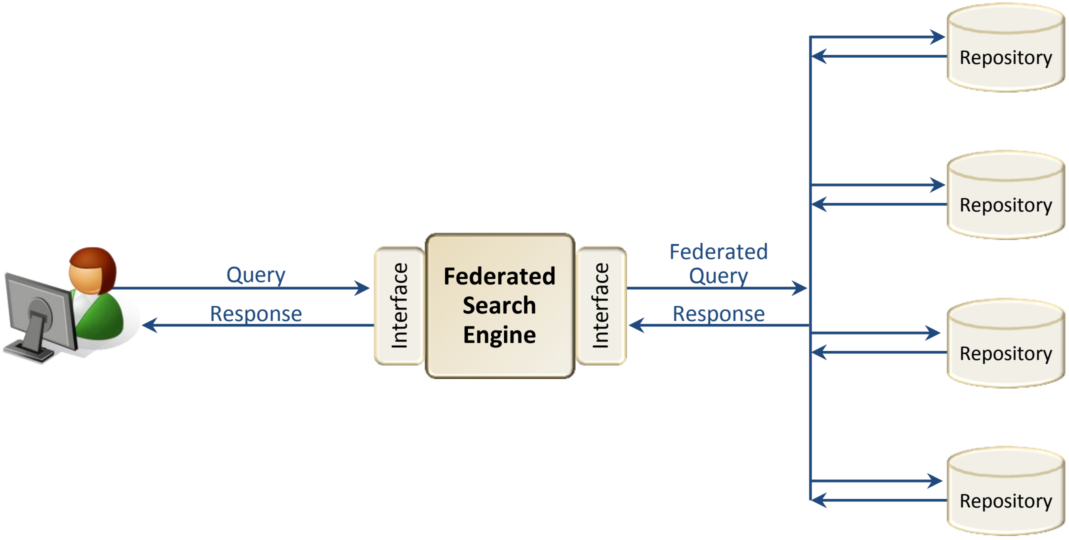


Figure 12. Federated Query Pattern

4 ISE I^2F ALIGNMENT TO ARCHITECTURE FRAMEWORKS

The ISE I^2F recognizes that ISE mission partners are aligned with different architecture frameworks, though the underlying concepts and principles may be very similar. These frameworks provide methodologies that enhance interoperability among diverse systems and data types to facilitate the transfer and exchange of necessary information. They align capabilities, competencies, and services in a way that is best defined for their specific communities. The ISE I^2F references these frameworks so that ISE participants can understand how the ISE I^2F interoperability requirements can be put in context of existing enterprise architecture efforts. The ISE I^2F provides a higher-level mechanism to align reference architectures, which provide more specific requirements associated with a specific service or capability. Overviews of the existing architecture frameworks are provided in Appendix A.

The intent of the ISE I^2F is not to drive convergence of architecture frameworks to one, but to foster alignment among these frameworks from an ISE interoperability perspective. OMB's Common Approach to Federal Enterprise Architecture (FEA), is available and ISE mission partners are already expected to align with the frameworks it outlines. The ISE normalizes these differences by describing interoperability needs, requirements, and alignment in the context of the Common Approach (CA). This meets the needs of stakeholders and participants described in Table 1, Core Participants.

4.1 COMMON APPROACH (CA) – ARCHITECTURE DOMAINS

The architecture domains articulated in the Common Approach to Federal Enterprise Architecture essentially describe the architecture domains used to support a variety of business and technical needs.

Figure 13 depicts the key components of the common approach, as defined within FEAF.

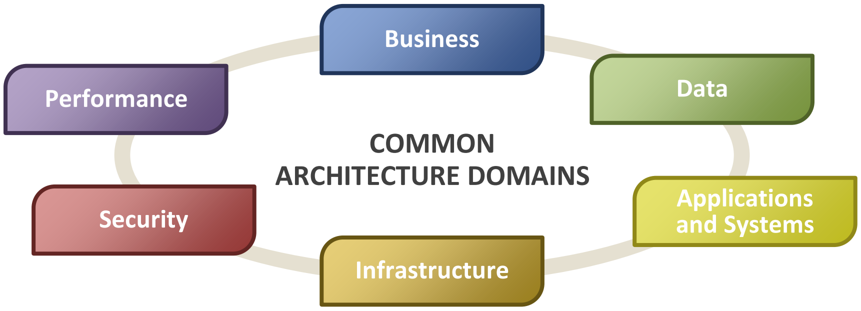


Figure 13. Common Approach Domains

4.2 ALIGNMENT OF COMMON APPROACH AND ISE I^{2}F

The following sub-sections provide a high-level description of the Common Approach domains—Business, Data, Applications and Systems, Infrastructure, Security, and Performance—and their applicability to the ISE I^{2}F.

4.2.1 BUSINESS DOMAIN

The business domain addresses business/mission objectives of a specific architecture or system effort. This section is most relevant to the Operational Capabilities section of the ISE I^{2}F. Areas within the business domain that would be applicable to address interoperability include:

- Alignment of ISE participant architectures to ISE relevant interoperability and information sharing policies and guidance,
- Mission vision, objectives, and requirements,
- Standards and approaches for capturing business requirements and modeling business processes and information flows,
- Lines of business, capabilities, and activities,
- Common information exchanges for a specific mission scenario/use case, and
- Capture information sharing requirements, constraints, and rules between partners.

4.2.2 DATA DOMAIN

In the data domain, the ISE I^{2}F plays a major role in defining the interoperability requirements. Relevant ISE I^{2}F context includes the relationship to the sections on exchange patterns, technical standards, technical capabilities, and exchange specifications. The data domain builds on the operational context mentioned earlier in this framework and defines why information needs to be exchanged. The exchange patterns abstract out the interoperability requirements and provide a foundation for how the exchange will be implemented. Technical standards are enablers that provide the vocabularies for sharing to assure that the semantic meaning and the context of the data is not lost during transition and transformation. Technical capabilities provide the architectural context within which the exchange is executed. All of these components focus on the abstracted interoperability framework. The actual data constructs for an information exchange are defined during the process of developing the exchange specification, where technical vocabulary standards are applied to define the data exchange content model and includes:

- Mechanism for identifying and categorizing candidate assets for sharing,
- Framework for capturing data elements and the relationship between them (semantics),
- How the data is structured, what standards are used, and how data/information can be exchanged so users are able to both have access to and use the data/information,

- Technical standards to design and implement information sharing capabilities into ISE systems,
- Approach for documenting exchange patterns,
- Data/information flow to include the tagging of the data, discovery, and retrieval, and
- Principles, roles, and responsibilities for data management and stewardship.

4.2.3 APPLICATIONS AND SYSTEMS DOMAIN

The applications and systems are part of the reference implementation context and should be addressed at the reference architecture level. However, the definition and alignment with exchange patterns during the process of specification development is a critical consideration for achieving interoperability. These considerations align to the international community of business analysts, developers, and architects, whereby the goal of *intrinsic interoperability*[49] is a fundamental concept and accomplished via the *service-oriented* design approach. This approach encompasses an evolution of design and development practices to achieve agnostic, componentized services as build once and reused many, e.g., service reusability, predictability, discoverability, abstraction, and standardized contracts.[50] Relevant ISE I^{2}F context includes exchange patterns and exchange specifications as described previously in sections 3.4, and 3.5 respectively. Applications and systems implications for interoperability include:

- Service standards and frameworks (e.g., service metadata and protocol standards, service-oriented architecture, standard application programming interfaces (APIs)),
- Specifications and functional requirements of the applications/services to the level necessary so external application developers can interface with applications/services, and
- Recommended and/or possible implementation approaches (e.g., cloud, SOA, mobile).

4.2.4 INFRASTRUCTURE DOMAIN

The infrastructure domain is a significant enabler in information sharing. While important to interoperability, infrastructure is localized to the sharing partner agencies, and should be addressed within the reference architecture sections or during the implementation phase. Architecture implications for interoperability include:

- Interfaces (protocols and interface standards) and networks making internal and external domains and applications/services interoperable,
- Flow or routing of information between network connections and/or across security fabrics/domains,

[49] Erl, Thomas. *Service-Oriented Architecture: Concepts, Technology, and Design.* Prentice Hall/Pearson PTR ISBN: 131858580.

[50] http://serviceorientation.com/serviceorientation/service_orientation_and_interoperability

- Practical design-patterns as groups of technology packets that work well together to support system deployment, and
- Standards, platforms, and products to increase interoperability across partners.

4.2.5 SECURITY DOMAIN

The security domain is where the ISE I^{2}F plays a major role in defining the interoperability requirements within and across multiple security enclaves. Relevant ISE I^{2}F context includes operational capability, exchange patterns, technical standards, technical capabilities, and exchange specifications. This domain also defines other key concepts around identity, access, and authorization of users to enable secure, authorized access to the right information. The operational context defines why information needs to be protected (security, privacy, classification, etc.). Further, the exchange patterns abstract out the interoperability requirements; provide a foundation for security requirements and demonstrate how the exchange may be implemented. Technical standards are enablers that provide the technology standards for safeguarding information at rest, and in motion. Technical capabilities provide the architectural context within which the exchange is executed and protected. This will include definition of data tagging at the endpoints and at the fine grain content level. Security implications for interoperability include:

- Proper security controls to ensure the protection of information as it is exchanged within and across security fabrics,
- Access authorization controls to protect shared data assets,
- Metadata to tag the data and describe its pedigree, lineage, source, timeliness, confidence, or other attributes associated with trust, and
- Digital security rules, guidelines, and standards for securely exchanging data and services.

4.2.6 PERFORMANCE DOMAIN

The performance domain addresses specific performance requirements among exchanging mission partners in alignment with mission priorities. These are often addressed at the actual implementation level. However, there may be some business sensitivities that will require these requirements to be addressed at the ISE I^{2}F level. Relevant ISE I^{2}F context includes operational capability.

4.2.7 COMMON APPROACH ALIGNMENT TO ISE I^{2}F

Interoperability requirements are defined and need to be addressed for each of the domains identified in the CA; and interoperability is achieved when requirements clearly articulate attributes for data, exchange mechanisms, and/or services. Table 3 delineates the minimum common architecture domain artifacts required for interoperability when utilizing existing architecture frameworks. The ISE I^2F focuses on driving the definition of common artifacts and concepts for information interoperability, with the expectation that domain-specific interoperability will be addressed as part of the reference architectures.

Table 3. ISE I^2F Operational Capability Alignment to the Common Approach to Federal Enterprise Architecture

COMMON APPROACH DOMAINS	ISE I^2F				
	Operation Capabilities	Exchange Patterns	Technical Standards	Technical Capabilities	Exchange Specifications
Business	✓	✓			
Data	✓	✓	✓	✓	✓
Infrastructure				✓	
Performance	✓				
Security	✓	✓	✓	✓	✓
Applications/Systems		✓	✓		✓

The ✓ marks indicate where there is some alignment between ISE I^2F Operational *Capabilities and the applicable Common Approach domain.*

The ISE I^2F recognizes that the ISE mission partners are aligned with different existing architecture frameworks. It may not be necessary to address all capabilities outlined in each domain of the common approach at the ISE I^2F level; some capabilities will be addressed as part of the reference implementation. Table 3 defines the initial alignment of the ISE I^2F and the common approach. Consistency in how ISE participants address these interoperability requirements within each domain will assist in coordinating activities to define the nationwide ISE capabilities.

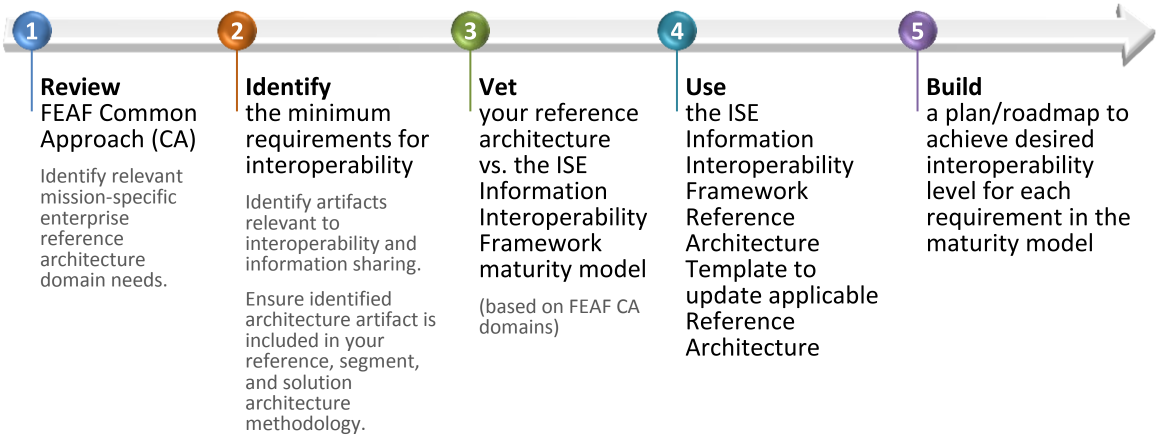
This page intentionally left blank.

5 BUILDING INTEROPERABILITY INTO MISSION-BASED ARCHITECTURE(S)

5.1 PROCESS OVERVIEW

ISE constituents can use the ISE I^{2}F Architecture Framework Alignment Grid and Reference Architecture Template to ensure that the applicable mission specific reference architecture includes information sharing capabilities based on standards specifications and promotes data exchange (via Common Profile).

Use the ISE I^{2}F Architecture Framework Alignment Grid, Interoperability Maturity Model, and Reference Architecture template to:



1 **Review** FEAF Common Approach (CA)

Identify relevant mission-specific enterprise reference architecture domain needs.

2 **Identify** the minimum requirements for interoperability

Identify artifacts relevant to interoperability and information sharing.

Ensure identified architecture artifact is included in your reference, segment, and solution architecture methodology.

3 **Vet** your reference architecture vs. the ISE Information Interoperability Framework maturity model

(based on FEAF CA domains)

4 **Use** the ISE Information Interoperability Framework Reference Architecture Template to update applicable Reference Architecture

5 **Build** a plan/roadmap to achieve desired interoperability level for each requirement in the maturity model

Figure 14. ISE I^{2}F Architecture Process

5.1.1 REVIEW FEAF CA

Review FEAF CA; align with the reference architecture methodology use in your environment.

The ISE I^{2}F aligns with the FEAF CA domains to outline the minimum artifacts for developing architecture interoperability. From the FEAF domains the ISE I^{2}F has captured interoperability requirements which are represented in each generally accepted architecture frameworks (DoDAF, GRA, IC PAG, TOGAF, etc.). These frameworks along with the suggested interoperability artifacts can be found in ISE I^{2}F Appendix B: Architecture Framework Alignment Grid.

5.1.2 IDENTIFY THE MINIMUM REQUIREMENTS FOR INTEROPERABILITY

The ISE I^{2}F uses the FEAF CA domains as a baseline to analyze architecture frameworks. From the domains identified in the FEAF CA, the I^{2}F has captured interoperability requirements which are to be represented of the artifacts in the generally utilized architecture frameworks (DoDAF, FEAF CA, TOGAF, etc.). These frameworks along with the suggested artifacts required for interoperability can be found in the Architecture Framework Alignment Grid in Appendix B. These artifacts from the Alignment Grid should be compared against your existing mission architecture which can be used as a basis in analyzing and identifying interoperability gaps when using the Maturity Model in the next step.

Review FEAF CA and the applicable reference architecture framework used to develop your architecture; identify policy and/or legal requirements that may constrain the solution space of the mission architecture; and identify *mission*- and *business*-specific enterprise reference architecture domain needs in each of the FEAF CA domains.

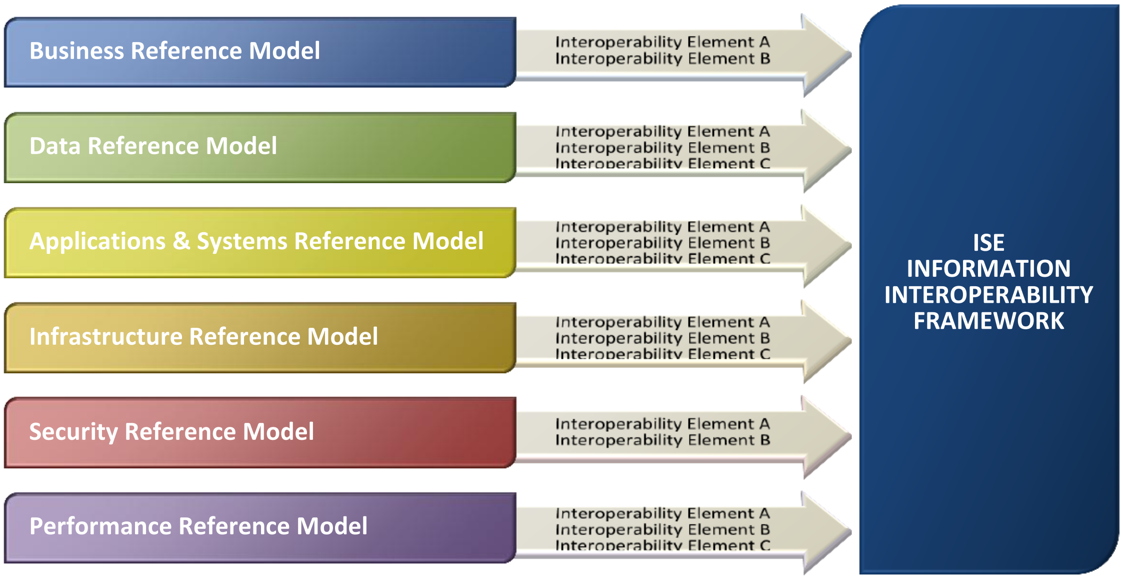

Business Reference Model
Interoperability Element A
Interoperability Element B
Data Reference Model
Interoperability Element A
Interoperability Element B
Interoperability Element C
Applications & Systems Reference Model
Interoperability Element A
Interoperability Element B
Interoperability Element C
Infrastructure Reference Model
Interoperability Element A
Interoperability Element B
Interoperability Element C
Security Reference Model
Interoperability Element A
Interoperability Element B
Performance Reference Model
Interoperability Element A
Interoperability Element B
Interoperability Element C
ISE INFORMATION INTEROPERABILITY FRAMEWORK

Figure 15. Reference Architecture Components

5.1.3 ISE I^{2}F MATURITY MODEL

Evaluate your mission reference architecture and interoperability architecture artifacts developed against the ISE I^{2}F maturity model in Appendix C. The ISE I^{2}F maturity model is broken down by FEAF CA domains (business, data, applications and systems, security, infrastructure, and performance) with characteristics established for each level of interoperability (ad hoc, repeatable, enhanced, managed, and optimized) for each interoperability requirement. For each element determine the maturity level of your mission architecture by moving across each row and matching your current state. During this step you should also note the characteristics of each requirement where the requirement/element maturity is less than your desired level (Ex., your interoperability level is at 'repeatable'; you need to be at 'managed'). Note that mission-specific architectures will have different goals for each element maturity level based on the operational needs or organizational policy of the mission architecture.

5.1.4 USE THE ISE I^2F REFERENCE ARCHITECTURE TEMPLATE TO UPDATE APPLICABLE MISSION REFERENCE ARCHITECTURE(S)

The ISE I^2F reference architecture (RA) template contained in Appendix D is designed to aid the development of reference architecture artifacts to support interoperability. For each of the FEAF CA domains, the template is a guide to the relevant interoperability requirements and artifacts to be incorporated for interoperability. The template details interoperability goals in each of the domains, as well as instructions for template usage.

The RA template contains an overview of the interoperability goals for each CA domain and the objectives of the artifacts within the domain. Within each domain listed, the RA template provides an overview of the information to be included in each artifact, and instructions on how to develop each interoperability artifact. Each domain is divided into subsets of the domain: For example, the CA business domain is divided into business processes; business models, mission exchange processes, diagrams and flows, other considerations, etc.

In addition, the RA template has been integrated with the Architecture Framework Alignment Grid with mnemonics mapping each item in the template to the applicable artifact reference in the Grid. When used in conjunction with the Architecture Framework Alignment Grid, the architecture framework can be updated to included interoperability in each domain.

Annually OMB will receive business and technology architecture information from each department/agency (D/A) in the form of a high-level, integrated description of the agency's IT-related strategic goals, business objectives, and enabling IT capabilities to include roadmaps. By leveraging the interoperability baseline provided by the Enterprise Architecture Maturity Measurement Template, OMB can more easily understand the D/As progress towards integrating interoperability requirements into their existing architectures while improving their abilities to fulfill strategic priorities.

5.1.5 BUILD A PLAN/ROADMAP TO ACHIEVE DESIRED INTEROPERABILITY LEVEL FOR EACH REQUIREMENT IN THE MATURITY MODEL

After completing the previous steps and determining which interoperability elements should be incorporated into each EA domain, build a plan and roadmap that leads to interoperability at the applicable maturity level for your mission specific EA. The plan and roadmap should address each interoperability requirement where improvement is deemed necessary. The roadmap should consider the availability of both intra- and inter-agency shared services which will require coordination.

The following graphic is provided to show the relationship between the Maturity Model Assessment (Appendix C), the Architecture Framework Artifact Build (Appendix B), the Reference Architecture Template Activity (Appendix D), and the building of the Interoperability Roadmap, as well as inputs and outputs of each activity. The Interoperability Roadmap build activity will also require the interoperability goals for the specific mission architectures since the maturity level (ad hoc, repeatable, enhanced, managed, or optimized) goals will be different for each mission architecture based on its needs.

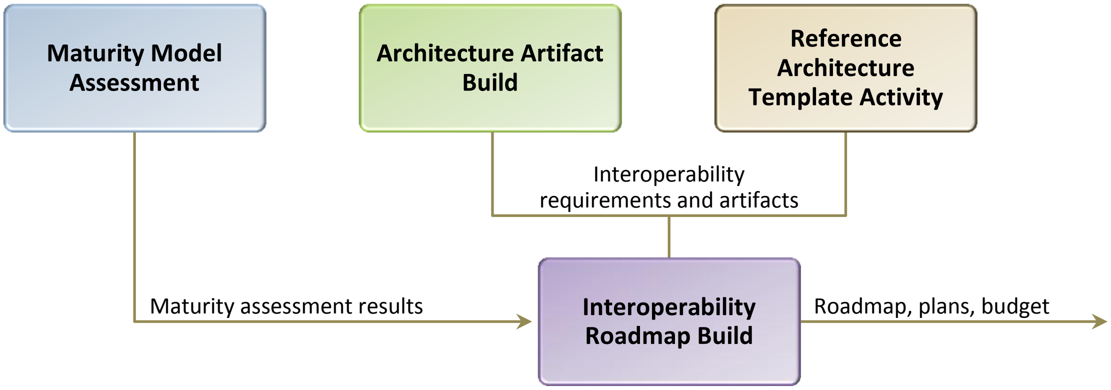

Maturity Model Assessment
Architecture Artifact Build
Reference Architecture Template Activity
Interoperability requirements and artifacts
Maturity assessment results
Interoperability Roadmap Build
Roadmap, plans, budget

Figure 16. Interoperability Architecture Build Activities

It would be advantageous to interoperability efforts if this roadmap/plan were maintained to monitor progress towards interoperability goals and to coordinate plans across departments and agencies. Options for monitoring include: 1) ISA IPC via the Senior Architect’s Forum, 2) OMB via E-Gov Initiative, 3) the Federal CIO Council.

6 ISE INDUSTRY STANDARDS AND SPECIFICATIONS FRAMEWORK

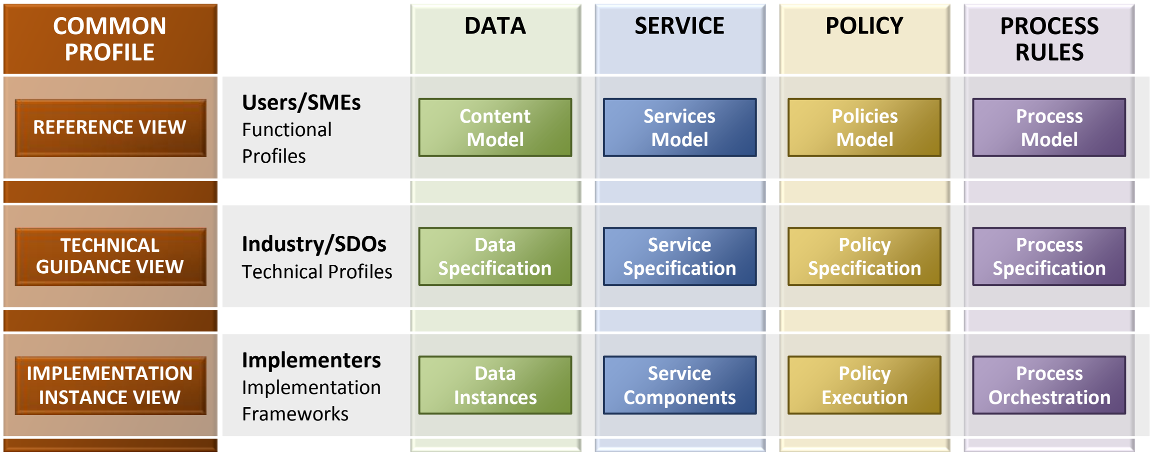
6.1 STANDARDS ANALYSIS

The convergence of information sharing capabilities and interoperability is essential to standards requirements analysis; as business needs and new technology may require standards that support the implementation of one or more information sharing capabilities.

The ISE Standards and Specifications Framework will:

- Define a framework for understanding standards, the function they serve, what stakeholders are involved, and the relationship between standards;
- Organize standards by function, stakeholder, and content;
- Identify frameworks of mutually supportive standards;
- Group existing and proposed standards by functional area; and,
- Create a model for standards frameworks.

The following section elaborates on this standards framework, and is also aligned with the ISE Common Profile. For information exchange to occur, there are typically four key components of that exchange (Figure 17).



COMMON PROFILE		DATA	SERVICE	POLICY	PROCESS RULES
REFERENCE VIEW	**Users/SMEs** Functional Profiles	Content Model	Services Model	Policies Model	Process Model
TECHNICAL GUIDANCE VIEW	**Industry/SDOs** Technical Profiles	Data Specification	Service Specification	Policy Specification	Process Specification
IMPLEMENTATION INSTANCE VIEW	**Implementers** Implementation Frameworks	Data Instances	Service Components	Policy Execution	Process Orchestration

Figure 17. Standards Framework Aligned to the Common Profile

6.2 FUNCTIONAL PROFILES

Functional profiles represent standards, mechanisms, and processes for consistent documenting and modeling of business requirements. These standards help better define requirements for functional and technical standards, and are useful in modeling these requirements. As the requirements and the associated models mature, this helps to identify and articulate commonality in requirements among communities of interest, and drive a meaningful discussion toward alignment with an eventual goal of convergence. This leads to national models where requirements are uniformly agreed upon, and these requirements form functional standards. Figure 18 provides an example of such a profile.

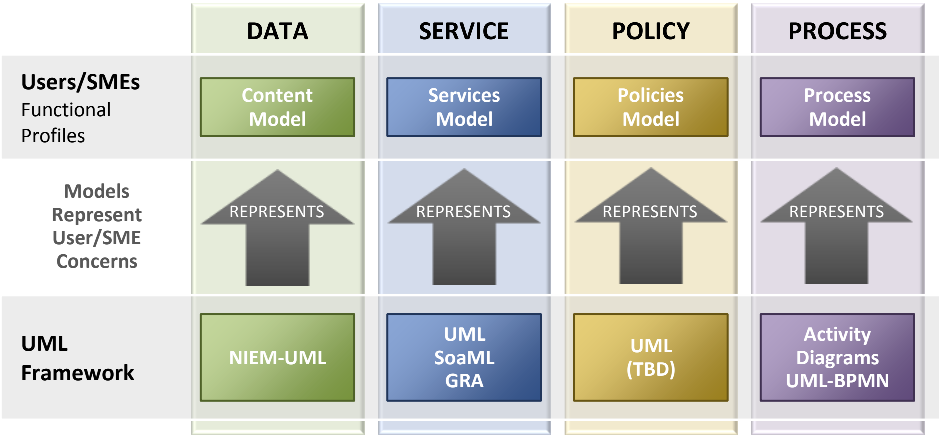


Figure 18. Example of a Functional Standards Profile

In this example, the UML framework is an example of coherent and mutually supportive sets of capabilities that satisfy the needs of a stakeholder group. The data component of this exchange will be NIEM, and NIEM UML profile-based modeling tools will be utilized to develop the requirements and associated models for this exchange. From a services perspective, in the justice and public safety community, the GRA is the prevalent standard adopted by the community to specify the services components of their exchange. While the GRA is a services specification, there is no associated model to really model these services. This identifies a gap in modeling tools that minimize manual development of the services specification.

On the policy aspects of this framework, there is no clearly defined standard. The justice and public safety community is starting the use their own Global Federated Identity and Access Management Framework; there is no tooling support for this standard. On the process side of this framework, there are tools available that offer support for process modeling, but no real profile that allows for developing domains models for justice and public safety.

6.3 TECHNICAL PROFILES

Technical profiles represent the actual technical standards developed by the standards development organizations, or derivatives of those standards that help address the functional requirements defined using the functional profiles. For a given set of functional profiles, there might be more than one technical profile that addresses the specific needs for that exchange. Figure 19 provides an example of such a profile.

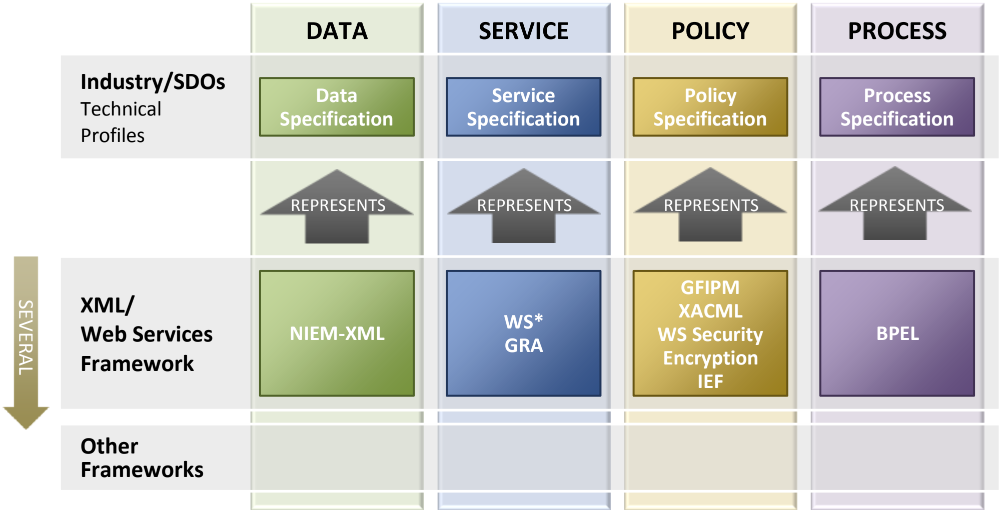
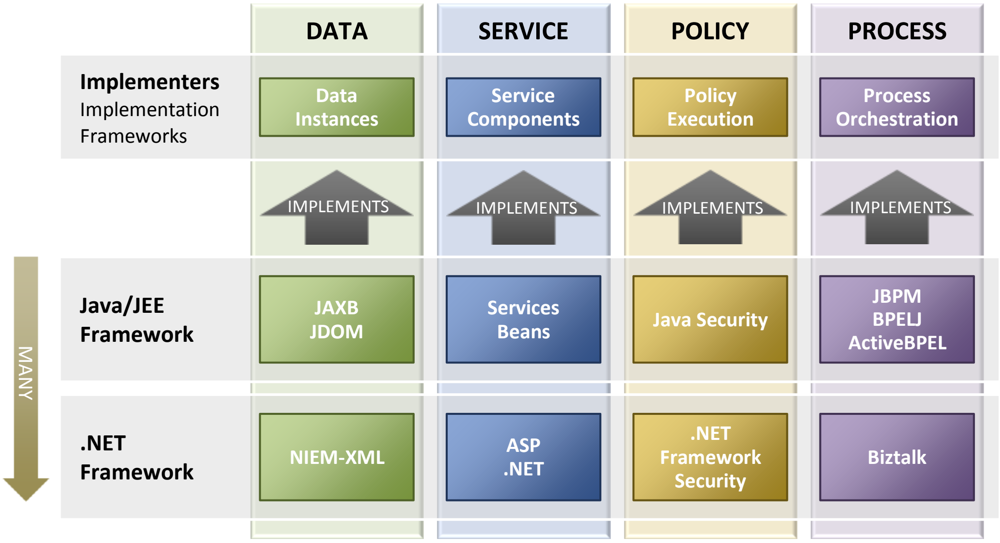


Figure 19. Example of a Technical Profile

In this example, the XML/web services framework is an example of coherent and mutually supportive sets of capabilities that satisfy the needs of a stakeholder group. The actual technical specification standard that powers NIEM is the W3C Schema Specification, which is also the normative representation for NIEM. Similarly, from a services perspective, the underlying technical specification for GRA is the WS* set of OASIS standards. If a practitioner has specific MQ-based asynchronous messaging requirements, there might be another option here for an MQ-based service specification. On the policy aspects of this framework, there are a number of options that might be used. The Global Federated Identity and Access Management Framework addresses identity policy requirements; there may also be a need to address privacy policies. There is no specific standard that addresses that today, but XACML is a solid alternative to help meet those requirements. On the process side of this framework, there are stable standards that help with process representations, but nothing specific to address the need for this domain. In this scenario, more than one technical profile addresses one functional framework.

6.4 IMPLEMENTATION PROFILES

Implementation profiles represent the actual reference implementations for the functional and technical profiles. Implementation profiles are instrumental in developing reference implementations that prove the functional and technical profiles. These implementations are often tool specific and driven by the internal development environments for the participating agencies.



	DATA	SERVICE	POLICY	PROCESS
Implementers Implementation Frameworks	Data Instances	Service Components	Policy Execution	Process Orchestration
	IMPLEMENTS	IMPLEMENTS	IMPLEMENTS	IMPLEMENTS
Java/JEE Framework	JAXB JDOM	Services Beans	Java Security	JBPM BPELJ ActiveBPEL
.NET Framework	NIEM-XML	ASP .NET	.NET Framework Security	Biztalk

Figure 20. Example of Reference for Functional and Technical Profiles

In this example, there might be two or more implementation profiles, but the most common ones in use are based on a JEE or .NET framework. The underlying tooling and development capabilities will also vary based on the framework. However, since the focus of the information sharing standards is primarily limited to the sharing of information in motion, the actual implementation almost becomes irrelevant.

7 INTEROPERABILITY AND USE OF THE COMMON PROFILE

7.1 ISE COMMON PROFILE FRAMEWORK DESCRIPTION

The ISE Common Profile Framework Description, known as the Common Profile, is an ISE tool that provides a structured but modular approach in describing a component to promote reuse, standardization, and interoperability across various subject areas and organizations. Simply put, a common profile is a set of instructions that describes how to achieve a desired outcome. Similarly, the Common Profile supports the mission and business needs across government organizations by identifying a base set of elements, specifications, and/or standards so that these organizations can become interoperable through sharing services and information resources. This is accomplished through documenting the mission/business requirements along with the supporting capabilities and the enabling technical modular components. Given a scenario – a community of interest made up of six organizations decides to implement a *Common Desktop Gateway* (business need) to foster employee mobility and cost avoidance across the community. In this scenario, it would be inefficient and challenging if each organization decides to implement operational and technical components, required in support of the business need, internal to their organizations, thereby achieving no interoperability or cost avoidance. A Common Profile helps avoid this siloed approach by leveraging a common methodology for referencing standards and specifications across multiple organizations. So, a profile for the *Common Desktop Gateway* would be developed with the consensus of all six organizations where the operational and technical components can interoperate to provide the users 'same look and feel', as well access to desired services across the community networks.

As the name suggests, a Common Profile is a structure that is accepted across an enterprise or multiple organizations. To be common, the profile follows a set governance process that validates profile structure and mandates its use to deliver a specific mission or business need across the enterprise. The profile, once completed, follows a change management process, similar to that of a living document, and must be discoverable across organizations sharing a common (mission or business) interest.

The Common Profile contains three views that are used to identify the mission or business need of the enterprise, along with operational and technical components to achieve that need. The Common Profile views are: Reference View, Technical Guidance View, and Implementation Instance View. These views are defined as follows:

- **Reference View:** Serves as the high-level abstract example or reference for the profiled enterprise component. It includes basic attributes, enterprise entities, and guidance information. The reference view is implementation independent, vendor independent, and sometimes technology independent. The reference view should contain applicable mission needs statements, use cases and reference architecture.

- **Technical Guidance View:** A set of one or more base standards, and where applicable, the definition of chosen classes, subsets, options, and parameters of those base standards necessary for establishing the behaviors of a particular function or enterprise component. The technical guidance view is vendor independent and includes basic attributes, enterprise entities, implementation references, guidance, and compliance information.
- **Implementation Instance View:** Portrays a specific instance of an implementation and defines discrete configurations and parameters for the given instance. It includes basic attributes, enterprise entities, compliance information, and specific methods and techniques. The implementation instance view may or may not be vendor independent. This is the most detailed and specific view of a profile.

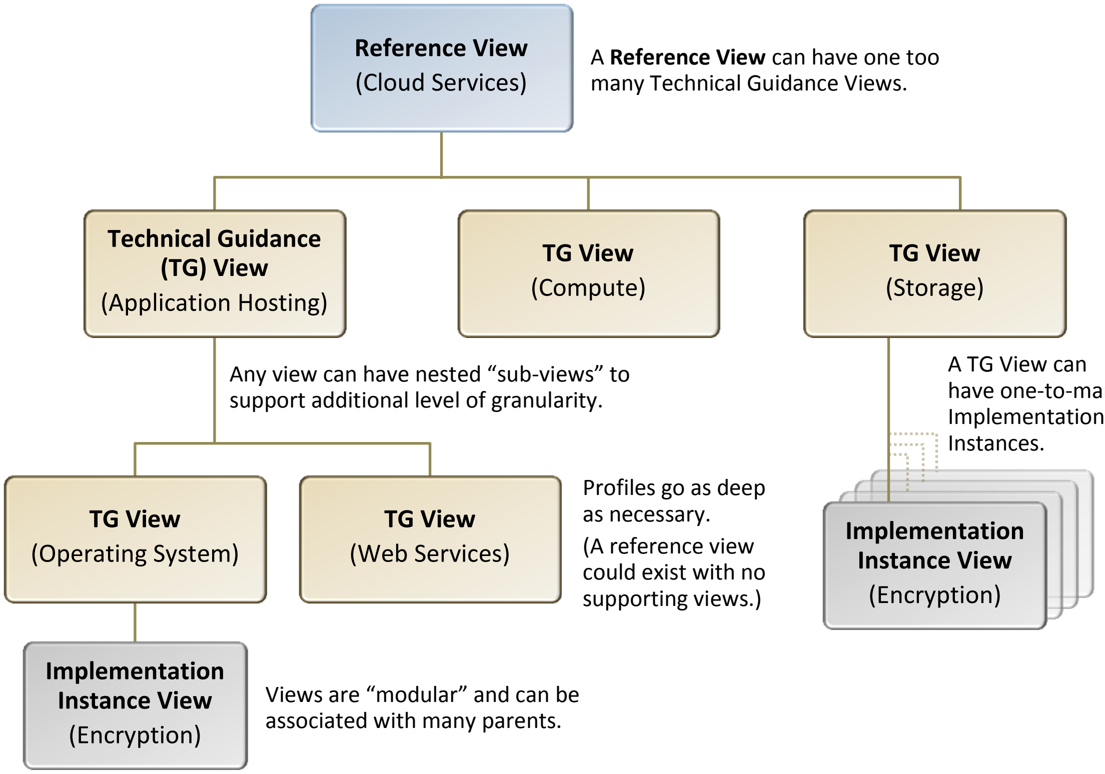

Reference View
(Cloud Services)
A Reference View can have one too many Technical Guidance Views.
Technical Guidance (TG) View
(Application Hosting)
TG View
(Compute)
TG View
(Storage)
Any view can have nested "sub-views" to support additional level of granularity.
A TG View can have one-to-many Implementation Instances.
TG View
(Operating System)
TG View
(Web Services)
Profiles go as deep as necessary.
(A reference view could exist with no supporting views.)
Implementation Instance View
(Encryption)
Implementation Instance View
(Encryption)
Views are "modular" and can be associated with many parents.

Figure 21 shows a conceptual profile called "Cloud Services"; it has three subordinate Technical Guidance Views (Application Hosting, Compute, and Storage). The Application Hosting View has subordinate (nested) Technical Guidance Views for Operating System and Web Services. An Implementation Instance View for Encryption supports two different Technical Guidance Views (Storage and Operating System). This example highlights the flexibility of the profile structure to adapt to particular needs.

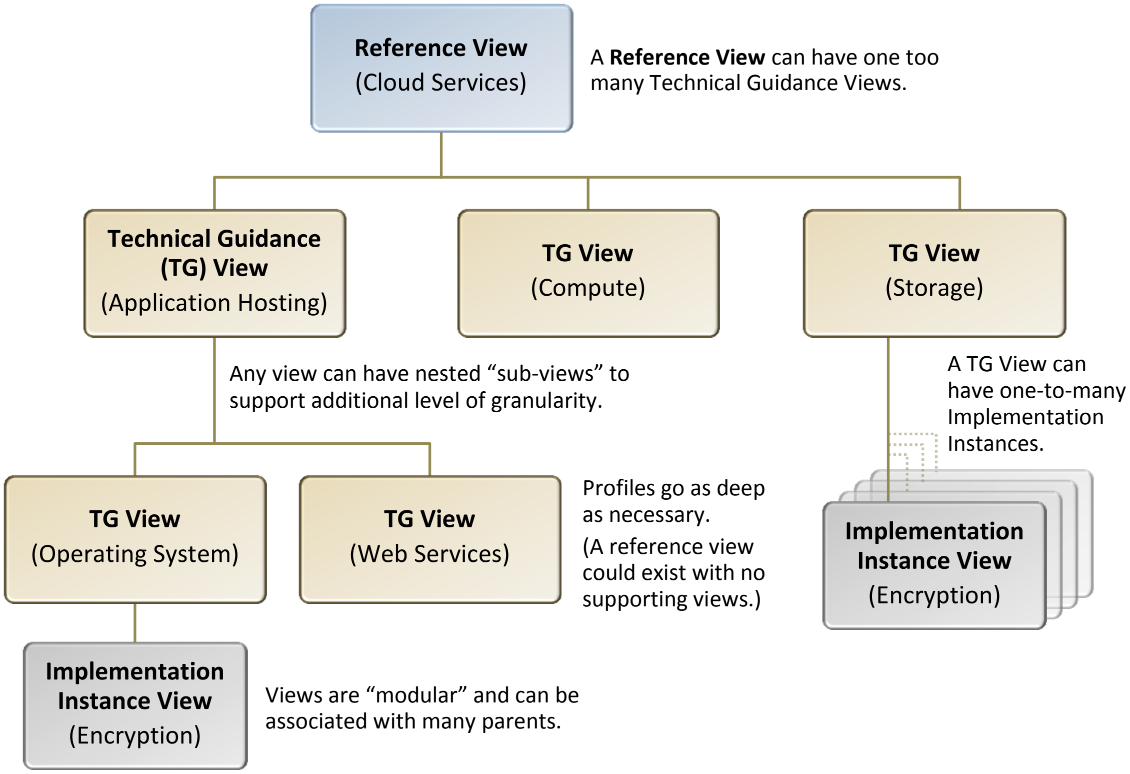

Reference View
(Cloud Services)
A Reference View can have one too many Technical Guidance Views.
Technical Guidance (TG) View
(Application Hosting)
TG View
(Compute)
TG View
(Storage)
Any view can have nested "sub-views" to support additional level of granularity.
A TG View can have one-to-many Implementation Instances.
TG View
(Operating System)
TG View
(Web Services)
Profiles go as deep as necessary.
(A reference view could exist with no supporting views.)
Implementation Instance View
(Encryption)
Implementation Instance View
(Encryption)
Views are "modular" and can be associated with many parents.

Figure 21. Profile Structure

The relationship between the Common Profile and the ISE I^{2}F is depicted in Figure 22.

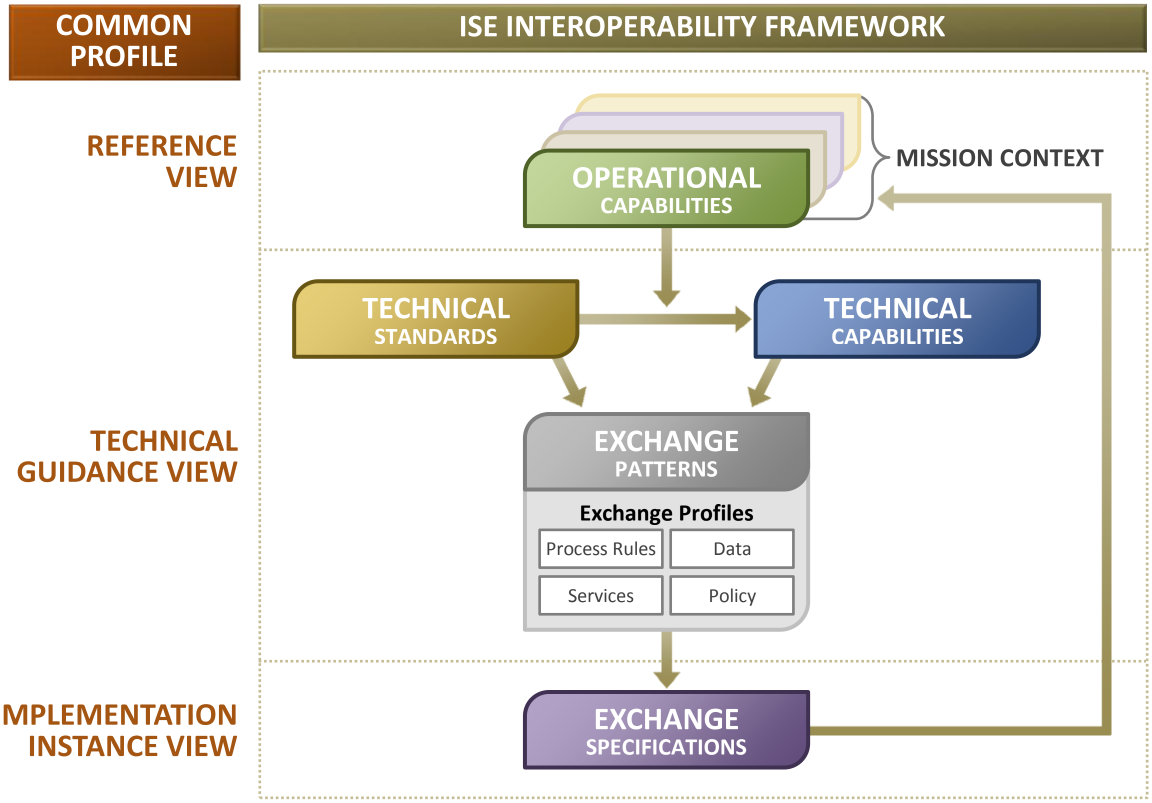


Figure 22. Common Profile and ISE I^{2}F Alignment

The following sections elaborate on the components of the ISE I^{2}F and how they align with the components of the Common Profile.

7.2 REFERENCE VIEW

The Reference View (Figure 23) elaborates on ISE I^{2}F operational capabilities by providing the basic attributes, enterprise entities, and guidance that is implementation independent, and focuses on describing the mission requirements.

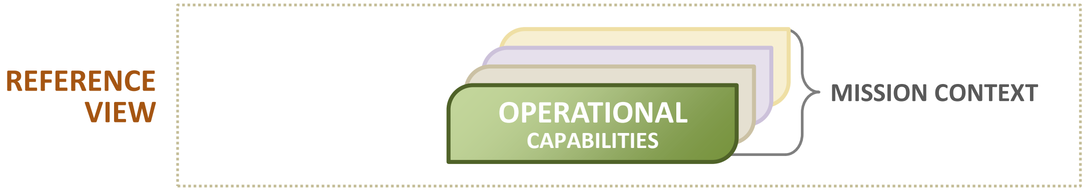


Figure 23. Reference View

7.3 TECHNICAL GUIDANCE VIEW

The Technical Guidance View (Figure 24) elaborates on ISE I^{2}F concepts around technical capabilities, technical standards, and exchange patterns. It is a set of one or more base standards, and where applicable, the definition of chosen classes, subsets, options, and parameters of those base standards necessary for establishing the behaviors of particular function or enterprise component. The technical guidance view is vendor independent and includes basic attributes, enterprise entities, implementation references, guidance, and compliance information.

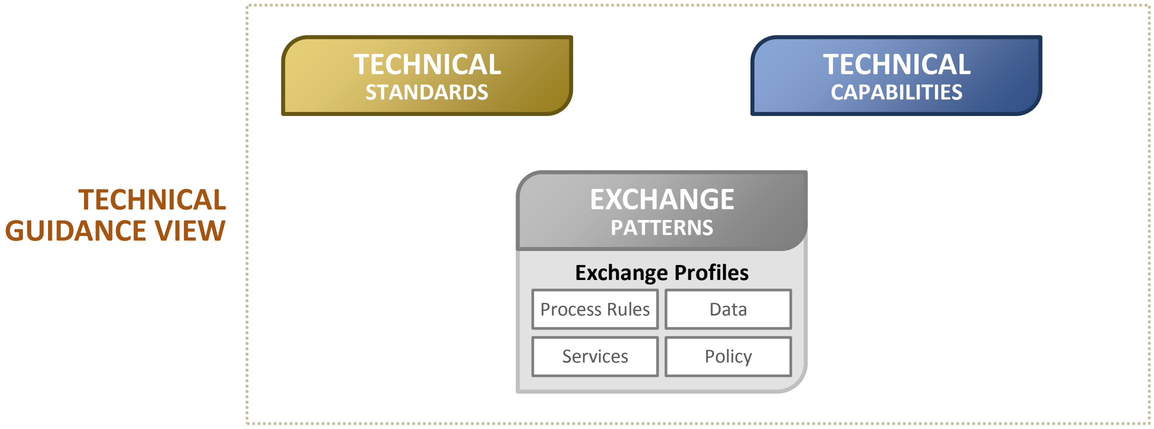


Figure 24. Technical View

7.4 IMPLEMENTATION INSTANCE VIEW

The Implementation Instance View (Figure 25) elaborates on ISE I^{2}F exchange specification area. This view focuses on a specific implementation instance and defines discrete configurations and parameters for the given instance. This view is critical as it allows an organization to tailor the technical implementation based on their existing configuration while still being interoperable through the use of Technical Standards. The parameters in this view include basic attributes, enterprise entities, compliance information, and specific methods and techniques. For example, if a Technical Standard is prescribed in the Technical Guidance View for Storage—a Technical Capability—then the configuration to implement that Technical Capability might vary from organization to organization. This variance can be based on type of storage hardware used or the encryption mechanism in a specific organization. The implementation instance view may or may not be vendor independent. This is the most detailed and specific view of a profile.

IMPLEMENTATION INSTANCE VIEW
EXCHANGE SPECIFICATIONS

Figure 25. Implementation Instance View

The content for these components are highly tailored based on the mission use case and capability needs. This builds on the high-level descriptions provided in Section 3.4.6, Exchange Profile. Process Rules, Data, Services, and considerations for the Common Profile are delineated in Table 4.

Table 4. Considerations for the Common Profile

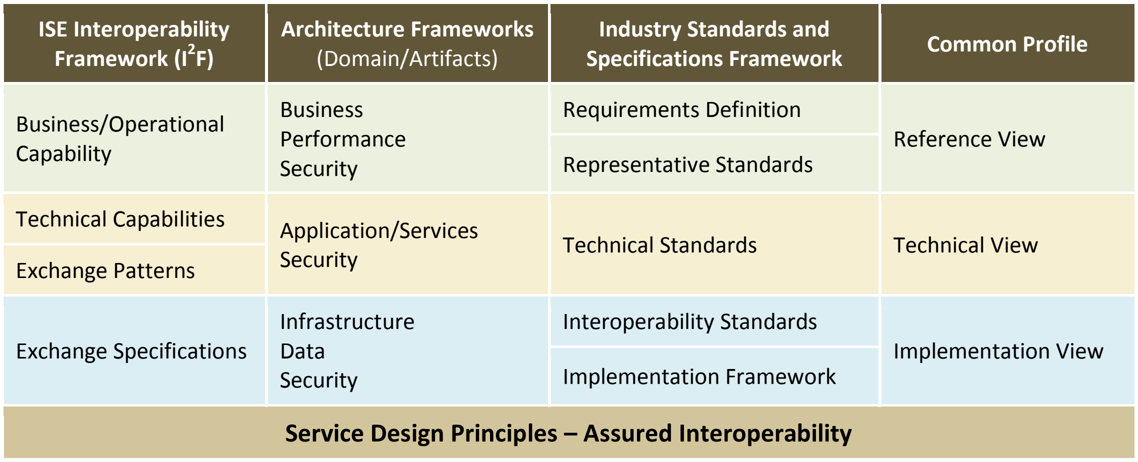
CONSIDERATIONS FOR THE COMMON PROFILE	MOST APPROPRIATE VIEW		
	R	TG	I
PROCESS RULES CONSIDERATIONS			
Detailed description and purpose of the exchange specification including the mission requirements, mission applications participating in the exchange, and any operational/policy considerations for exchanging, using, and disseminating data	R		
Key stakeholders and exchange partners, and their roles and contact information	R		
Change management process (if available)	R		
Role this exchange plays in a broader business capability—when and how to use this exchange	R		
What this exchange is, and is not	R		
How to extend or reuse this specific exchange, without losing the semantic meaning of the content or compromising baked-in interoperability requirements		TG	
Description of rules enforced in the specifications, along with key value lists applicable to this exchange			I
Description of applicable rules not enforced in the specification (and implementation guidance, if available, providing a clear explanation of how these rules need to be implemented when the exchange is implemented)		TG	
Descriptions of any shared services that might be used in processing the exchange, and mechanisms/links on how to access and use the service, MOUs that might be needed, and contact information for service owners			I
DATA CONSIDERATIONS			
Data elements and definitions that describe the data to be shared		TG	
Data model that may describe the structure of the data model			I
Business rules that may be applicable to the entire data set, or specific data elements		TG	
Based on a data vocabulary, identify any data mappings that may be required between the mission data, and appropriate elements in the vocabulary		TG	
Actual exchange model for the data			I
If an XML-based vocabulary is used, like NIEM, this data section of the specification will equate to an IEPD that will include all the descriptive sections and an XML schema (the normative specification)		T	
Based on the maturity of the exchange partners, mission need, and availability of a standardized methodology for data tagging, there may be additional requirements for tagging specific data elements			I
If a standardized methodology is not available, then the rules for tagging are often documented and may be implemented in the interface implementation			I
SERVICES CONSIDERATIONS			

CONSIDERATIONS FOR THE COMMON PROFILE	MOST APPROPRIATE VIEW		
	R	TG	I
Type of service – this will include information explaining if the service is synchronous, asynchronous, point-to-point, or multiple endpoints, etc. (certain architecture and implementation decisions are driven based on this information)		TG	
Number of endpoints			I
Description of endpoints – explanation of the type of endpoints and system components that will be participating in the exchange			I
Connection protocols – SOAP web services, RESTful services, queues, etc.			I
Connection parameters, including IP addresses, security/identity assertions, etc.			I
Metadata for service discovery (based on standardized taxonomy, if available)		TG	
Methodology and standardized tags for metadata tagging for the service specification to indicate identity and access management, security classifications, privacy and civil liberties, use and dissemination, provenance, etc. (if available and applicable)		TG	
POLICY CONSIDERATIONS			
Description of applicable policies and any available taxonomies/executable formats for the policy that may be used to automate/enforce the policy rules		TG	
Rules for how tags may be applied, including inter-dependencies, sequencing, and application of these rules		TG	
Processing rules and instructions for policy enforcement to be applied in the runtime environment		TG	
Describe what policies and rules will be enforced in the specification vs. need to be enforced in code during implementation			I

8 WAY FORWARD

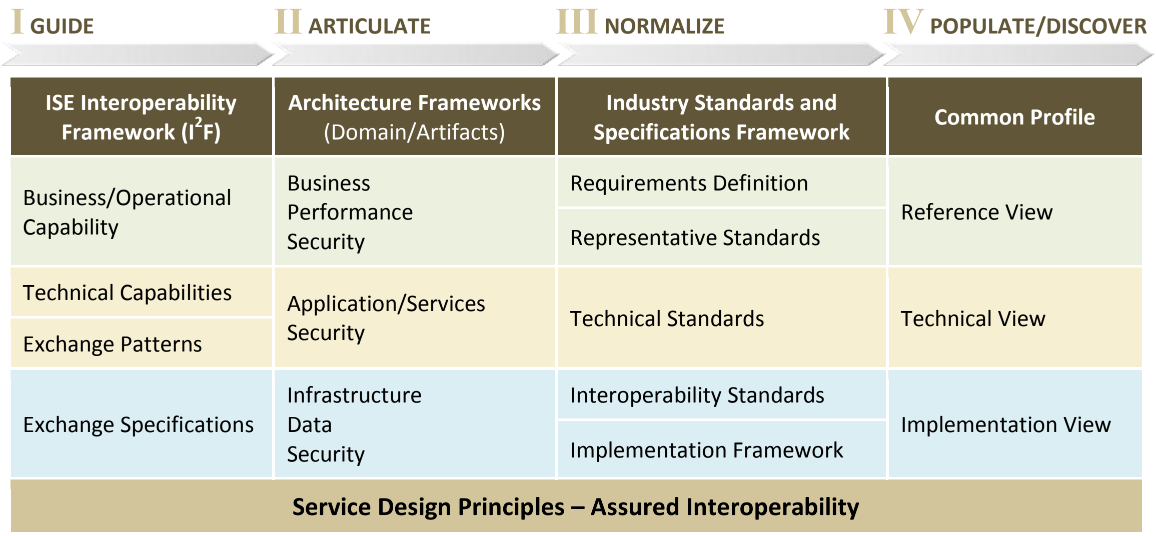
The main components of the ISE I^2F are: 1) **Business/Operational Capability**, 2) **Technical Capabilities**, 3) **Exchange Patterns**, and 4) **Exchange Specifications**. These components support a holistic approach for **discovering**, **building**, and **extending** interoperability services and requirements for internal mission needs, as well as for other external partners and interest. This is achieved through the use of ISE tools as IT management disciplines (e.g., ISE Architecture Framework Alignment Grid, ISE Standards and Specifications Framework, and ISE Common Profile adoption). The detailed Architecture Reference Template and Use Case help provide context and mission support guided by the ISE I^2F process.

Executives are provided authoritative language, interoperability concepts, and requirements aligned to national priorities for information sharing and safeguarding; this represents a way forward to implement internal policy, as well as prioritize investments. Project and program managers are supported through clearly outlined interoperability benefits, requirements, and implementation guidance through use cases, and business and technical views as best practices to develop metrics and performance measurements to achieve investment goals. Also, the ISE I^2F provides a well-defined roadmap through architecture and standard frameworks to extend interoperable capability to shared-service implementations, such as cloud or mobile platforms, and/or external partners. Architects, developers, and vendors receive ample support through artifacts and guidance that embraces the fundamentals of service-oriented and model-driven functional standards, and design principles, guiding reuse of agnostic, interoperable services and capabilities. Finally,



ISE Interoperability Framework (I^2F)	**Architecture Frameworks** (Domain/Artifacts)	**Industry Standards and Specifications Framework**	**Common Profile**
Business/Operational Capability	Business Performance Security	Requirements Definition	Reference View
		Representative Standards	
Technical Capabilities	Application/Services Security	Technical Standards	Technical View
Exchange Patterns			
Exchange Specifications	Infrastructure Data Security	Interoperability Standards	Implementation View
		Implementation Framework	
Service Design Principles – Assured Interoperability			

Figure 26 provides a view of the ISE I^2F aligned to the Common Architecture Domains, Common Profile, and Industry Standards and Specification Framework.



I GUIDE	II ARTICULATE	III NORMALIZE	IV POPULATE/DISCOVER
ISE Interoperability Framework (I^2F)	**Architecture Frameworks** (Domain/Artifacts)	**Industry Standards and Specifications Framework**	**Common Profile**
Business/Operational Capability	Business Performance Security	Requirements Definition Representative Standards	Reference View
Technical Capabilities Exchange Patterns	Application/Services Security	Technical Standards	Technical View
Exchange Specifications	Infrastructure Data Security	Interoperability Standards Implementation Framework	Implementation View
Service Design Principles – Assured Interoperability			

Figure 26. ISE I^2F Integrated Landscape

This page intentionally left blank.

APPENDIX A: ARCHITECTURE FRAMEWORK DESCRIPTIONS

FEDERAL ENTERPRISE ARCHITECTURE FRAMEWORK (FEAF), VERSION 2

The Federal Enterprise Architecture Framework, Version 2, describes a suite of tools to help government planners implement the Common Approach. At its core is the Consolidated Reference Model (CRM), which equips the Office of Management and Budget (OMB) and other Federal agencies with a common language and framework to describe and analyze investments. FEAF consists of a set of interrelated "reference models" that describe the six sub-architecture domains in the framework: Strategy, Business, Data, Applications, Infrastructure, and Security models. The use of these models and their applicability to interoperability are used to show the relationships between the capabilities demonstrated in each of the models.

DEPARTMENT OF DEFENSE ARCHITECTURE FRAMEWORK (DoDAF)

The interoperability frameworks provided within the current version of the DoDAF are utilized from the DoDAF interface and data models to suggest methods for enhancement in the exchange of information and data types. The exchange of information should enhance the capability of analysts and investigators to discover and access necessary information. DoDAF version 2.02 has capability, data, service, operational, and standards models and viewpoints that help architects and planners collect and view enterprise information in an integrated way. The specific DoDAF artifacts used depend on the scope and level of detail needed to be captured, although there are some artifacts that are typically always developed in the set of artifacts such as an OV-1, which provides an overview graphic along with a narrative description of the enterprise to be described.

GLOBAL REFERENCE ARCHITECTURE (GRA)

The GRA offers guidance on the design, specification, and implementation of services and related infrastructure as part of a justice service-oriented architecture (SOA). The GRA is an abstract framework for understanding significant components and the relationships between them within a SOA construct. It lays out common concepts and definitions as the foundation for the development of consistent SOA implementation. It is a description of the important concepts in an information sharing architecture and the relationships between those concepts.

INTELLIGENCE COMMUNITY (IC) ARCHITECTURE PRINCIPLES

Within the Intelligence Community (IC), the architecture frameworks and models are comprised of service lists, competencies, and a technical taxonomy model which relate to each other and is a way of looking at current and desired capabilities in a way to avoid, unless necessary, duplication of capabilities. The technical taxonomy breaks down technical services in a generic manner much like the Open Systems Interconnection (OSI) stack spells out the various components required in the delivery of a capability, such as applications, frameworks, data, hardware, networks, and facilities. The IC taxonomy model also has three higher layers—for governance and policy, capabilities, and services, showing the relationship and drivers for each instantiation within the taxonomy models and other supporting IC models.

Intelligence Community Joint Architecture Reference Model (IC JARM) and Program Architecture Guide (IC PAG): The IC JARM represents the IC's extension to the FEA CRM. It is comprised of an Enterprise Competency Model (ECM), Enterprise Services List (ESL), and Technical Services Taxonomy (TST). These are an interlinked set of clearly defined concepts produced by a body of experts in order to encourage clear communication and consistent description and analyses of investments and enhance intra-agency and inter-agency collaboration. The IC PAG is modeled from DoDAF and prescribes a set of consistent, viewpoint based artifacts at select points in the initiative's life cycle.

Other activities ongoing within the Intelligence Community are IC Core and IC Information Technology Enterprise (ITE). IC Core is a reference architecture intended to depict the ability of the IC to store, discover, collaborate, and provide security access to data within the IC in order to share data among a diverse user community. IC Core includes a "platform-as-a service" concept, which allows services to be shared throughout the community. IC ITE concepts such as the use of the cloud, collaborative tools, and common desktop environments were used in this document for their applicability to interoperability

THE OPEN GROUP ARCHITECTURE FRAMEWORK (TOGAF)

TOGAF is a framework for an enterprise architecture which provides a comprehensive approach for designing, planning, implementing, and governing enterprise information architecture. TOGAF is a high-level and holistic approach to design, which is typically modeled at four levels: Business, Application, Data, and Technology. It provides a well-tested foundational model to information architects. TOGAF relies heavily on modularization, standardization, and already existing, proven technologies and products, and supports loosely coupling and interoperability of services. (Also applicable, the Open Group has published three SOA standards and one SOA guide: *The Open Group Service Integration Maturity Model*, *The Open Group SOA Governance Framework*, *The Open Group SOA Ontology*, and the *Guide to Using TOGAF to Define and Govern SOAs*. The Open

Group has also published a white paper, *Navigating the SOA Open Standards Landscape around Architecture*, which was written by the Work Group together with members of OASIS and the OMG.)

APPENDIX B:
ARCHITECTURE FRAMEWORK ALIGNMENT GRID

This Architecture Framework Alignment Grid ("the alignment grid") details alignment of the ISE I^2F to reference architecture frameworks to achieve operational capabilities. The Architecture Framework Alignment Grid was developed to ensure interoperability alignment and inclusion in current architecture reference models and frameworks. This grid aligns each of the Common Approach domains (Business, Data, Applications and Systems, Infrastructure, Security, and Performance) with interoperability requirements, the ISE I^2F artifact (which provides a description of *how* it addresses the interoperability requirements), and the corresponding architecture artifact from each of the commonly accepted architecture frameworks (FEAF, DoDAF, TOGAF, GRA, and IC PAG).

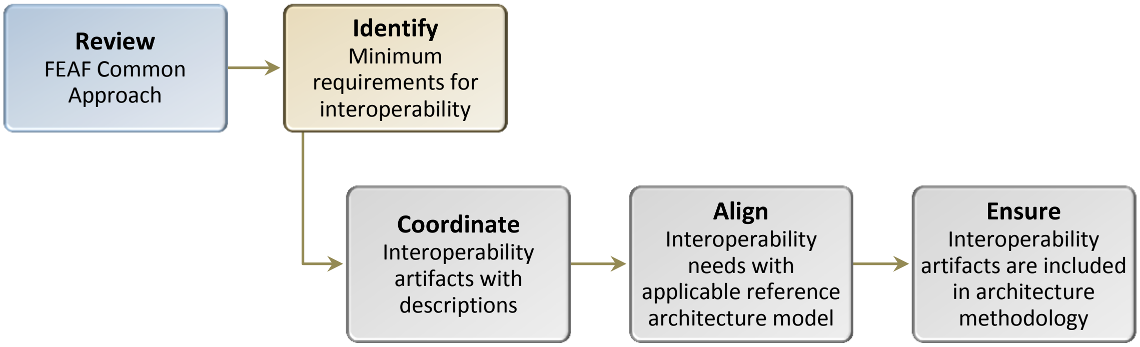
The alignment grid is designed to aid an implementer in the generation of the necessary architecture products based on the architecture framework required. The grid is sub-divided by the CA domains described above. The grid column definitions are:

- Column 1 – ISE I^2F **Minimum Requirements for Interoperability:** A description of the requirements in each of the domains needed to be interoperable.
- Column 2 – ISE I^2F **Artifact Description:** Provides instructions and recommendations on how to demonstrate interoperability based on the associated ISE I^2F requirement and using the selected frameworks on the right of the chart on the next page.
- Column 3-7 – **Applicable Architectural Artifacts:** Based on which architectural framework (FEAF, DoDAF, GRA, ICEA PAG, or TOGAF) is utilized, the artifacts for each framework are listed that address both the ISE I^2F requirements and ISE I^2F artifact description in the left columns of the chart on the next page.

The alignment grid is meant to address the gaps between business and technical stakeholders, providing architecture development guidance, artifact identification, and implementation support. It describes the minimum set of reference architectural artifacts necessary to demonstrate interoperability. The grid is also designed to aid an implementer in the generation of the necessary architecture products based on the architecture framework required.

For the Architecture Alignment and Implementation Process:

1. Review and identify mission- and business-specific enterprise reference architecture (i.e., Common Approach) domain needs. (Column 1)
2. Once mission and business needs are identified, review the minimum requirements for interoperability (e.g., what needs to be satisfied for your mission/business to be interoperable?). (Coordinate Columns 1 and 2)
3. Coordinate with interoperability artifact descriptions. (Identify descriptions in Column 3 that satisfy interoperability needs identified in Columns 1 and 2.)
4. Once interoperability needs are identified, align with applicable architecture artifact for methodology used at your department, agency, or business. (Select representative architectural reference model in Column 4; identify artifacts relevant to interoperability and information sharing.)
5. Ensure identified applicable architecture artifact is included in your reference, segment, and solution architecture methodology.



Review FEAF Common Approach

Identify Minimum requirements for interoperability

Coordinate Interoperability artifacts with descriptions

Align Interoperability needs with applicable reference architecture model

Ensure Interoperability artifacts are included in architecture methodology

NOTE: *Only one architecture framework (e.g., FEAF, DoDAF, GRA, IC PAG, or TOGAF) should be selected when developing the required architecture artifacts based on the organization. Also, please see Appendix D for a Reference Architecture Template, which includes detailed information on what to include when building or updating a reference architecture using the ISE I²F concepts for interoperability.*

ISE INFORMATION INTEROPERABILITY FRAMEWORK (I^{2}F)		APPLICABLE ARCHITECTURAL ARTIFACTS Applicable view, artifact, etc. – which maps to applicable reference artifact				
MINIMUM REQUIREMENTS FOR INTEROPERABILITY	ARTIFACT DESCRIPTION[51]	FEAF	DoDAF/UAF	GRA Service Specification Package, v1.0.0	IC-related (based on ICEA PAG)	TOGAF
BUSINESS DOMAIN						
Alignment of ISE participant architecture capabilities to ISE relevant interoperability and information sharing policies and guidance	• (B1) Describe the operational concept to be achieved • (B2) Provide the overall vision in a strategic context for the capabilities and a high-level scope • (B3) Provide a hierarchy of capabilities along with a description of the capabilities • (B4) Show the planned achievement of the capabilities by time frames and what constrains/policies are being applied	• Business Operating Plan • Business Service Catalog • Concept Overview Diagram • Strategic Plan	• CV-1: Vision • CV-2: Capability Taxonomy • CV-3 Capability Phasing or PV-2 Project Timelines (for Portfolio Management) • OV-1: High-level Operational Concept Graphic	• Business Process Models • Capabilities • Provisioning Model	• Operational Concept Description • Capability Description • Capability Taxonomy • Enterprise Guidance Matrix	• Phase A: Architecture Vision, Scope, Stakeholder Management, Communications Plan • Phase B: Business Architecture, Baseline Descriptions, Business Models, Information Exchange Matrix, Business Node Activities
Standards and approaches for capturing business requirements and modeling business processes and information flows	• (B5) Capture business requirements, preferably using standards from organizations (NIST, IEEE, ISO, etc.) that enable enterprise architecture models and analysis with regard to likewise comparisons between lines of business and organizations • (B6) Describe the information exchanges and their attributes • (B7) Document the data requirements and the structural business process rules	• Business Process Diagram) • Logical Data Model	• DIV-2: Logical Data Model • OV-2: Operational Resource Flow Description • OV-3: Operational Resource Flow Matrix • OV-5b: Operational Activity Model	• Enterprise Integration Patterns	• Activity Business Process Diagram • Operational Concept Description • Logical Data Model • Information Resource Flow Description • Information Resource Flow Matrix	• Business Process Models, Node Connectivity Diagrams, Information Exchange Matrix
Considerations for Information Sharing Agreements (ISAs)	(B8) Document the relevant ISAs and how these affect the exchange of information between users	• Business Process Diagram	• OV-2: Operational Resource Flow Description • OV-3: Operational Resource Flow Matrix • OV-6a: Operational Rules Model	• Information Model • Message Exchange Patterns	• Information Resource Flow Description • Operational Rules Matrix • Enterprise Guidance Matrix	• Activity Models, Service Levels, Boundaries and Contracts

[51] How it addresses interoperability requirement.

ISE INFORMATION INTEROPERABILITY FRAMEWORK (I^2F)		APPLICABLE ARCHITECTURAL ARTIFACTS Applicable view, artifact, etc. – which maps to applicable reference artifact				
MINIMUM REQUIREMENTS FOR INTEROPERABILITY	ARTIFACT DESCRIPTION[51]	FEAF	DoDAF/UAF	GRA Service Specification Package, v1.0.0	IC-related (based on ICEA PAG)	TOGAF
Exchange Specifications and their relation to technical standards and services within a specific mission context.	(B9) Provide the exchange specifications as they relate to the services, to include applicable technical standards from accepted standards bodies (ISO, IEEE, NIST, NIEM)	• Technical Standards Profile	• StdV-1 Standards Profile	• Service Interaction Profiles	• Relevant Mandated Standards	• Architecture Definitions, Architecture Requirement Specifications
DATA DOMAIN						
Mechanism for identifying and categorizing candidate assets for sharing	(D1) Provide the high-level data concepts and their relationships	• Knowledge Management Plan • Data Asset Catalog • Provider-to-Consumer Matrix	• DIV-1: Conceptual Data Model	• Domain Vocabulary	• Conceptual Data Model	• Phase C: Information Systems Architecture – Data • Application Principals, Data Principals
Framework for capturing data elements and the relationship between them (semantics)	(D2) Document the data requirements and their relationships, as well as the structural business process rules and metadata where necessary	• Logical Data Model	• DIV-2: Logical Data Model	• Message Definitions Mechanism	• Logical Data Model	• Architecture Definitions Document
Approach for documenting exchange patterns	(D3) Show the repeatable set of tasks that help accomplish the commonly occurring need for exchange of data/information between exchanging partners, as well as the data relationships and how the data relates to the business activities and their rules/policies	• Business Process Diagram • Logical Data Model • Data Flow Diagram	• OV-5b: Operational Activity Model • DIV-1: Conceptual Data Model • DIV-2: Logical Data Model • OV-3: Operational Resource Flow Matrix • OV-2: Operational Resource Flow Description	• Message Exchange Patterns	• Activity Diagram • Conceptual Data Model • Logical Data Model • Information Resource Flow Description • Information Resource Flow Matrix	• Activity Model • Baseline and Target Data Descriptions • Information Exchange Matrix
Principles and roles and responsibilities for data managements and stewardship	(D4) Show organizational relationships with respect to the data and its lifecycle	• Knowledge Management Plan	• OV-4: Organizational Relationships Chart (along with narrative)		• Operational Concept Description	• Data Management, Data Migration, and Data Governance
Technical standards to design and implement information sharing capabilities in ISE systems	(D5) Provide any necessary or relevant data standards to be considered for interoperability	• Technical Standards Profile	• StdV-1 Standards Profile		• Relevant Mandated Standards	

ISE INFORMATION INTEROPERABILITY FRAMEWORK (I^{2}F)		APPLICABLE ARCHITECTURAL ARTIFACTS Applicable view, artifact, etc. – which maps to applicable reference artifact				
MINIMUM REQUIREMENTS FOR INTEROPERABILITY	ARTIFACT DESCRIPTION[51]	FEAF	DoDAF/UAF	GRA Service Specification Package, v1.0.0	IC-related (based on ICEA PAG)	TOGAF
APPLICATIONS AND SYSTEMS DOMAIN						
Technical services supporting the common activities used for discovering, identifying, distributing, protecting, and managing information	• (A1) Identify services and common activities, their service components, and the interconnections between the services, as well as the data asset being exchanged • (A2) Provide a description of the data asset exchanged between services • (A3) Describe the functions performed by the services and the service data flows among the service functions • (A4) Describe the details of the data flows being exchanged between services and the attributes of the exchanges • (A5) Describe the resource/data flows between operation activities; this will be transformed to the flows between services	• Application Interface Diagram • Application Communication Diagram • Application Data Exchange Matrix • Data Flow Diagram	• SvcV-1 Services Context Description • SvcV-2 Services Resource Flow Description • SvcV-4 Services Functionality Description • SvcV-6 Services Resource Flow Matrix • OV-2: Operational Resource Flow Description	• Interface Description Requirements • Service Interfaces	• Service Component View • Interaction Diagram View • Interaction Matrix • Service Sequence	Phase C: • Information Systems Architecture – Applications • Application Portfolio Catalogue • Interface Catalogue • Application Organization Matrix • Application Role Matrix • Application Function Matrix • Application Interface Diagram • Application Communication Diagram • Application and User Diagrams • Application Location Diagrams • Process Application Diagram • Application Use Case Diagrams • Software Engineering Diagram • Software Distribution Diagrams
Developing service standards including service metadata, protocol standards, service oriented architecture, and standard APIs	• (A6) Document the service standards to be used by the services and applications	• Technical Standards Profile	• StdV-1 Standards Profile		• Relevant Standard Matrix	• Application Function Matrix • Application Interaction Matrix

ISE INFORMATION INTEROPERABILITY FRAMEWORK (I^2F)		APPLICABLE ARCHITECTURAL ARTIFACTS Applicable view, artifact, etc. – which maps to applicable reference artifact				
MINIMUM REQUIREMENTS FOR INTEROPERABILITY	ARTIFACT DESCRIPTION[51]	FEAF	DoDAF/UAF	GRA Service Specification Package, v1.0.0	IC-related (based on ICEA PAG)	TOGAF
INFRASTRUCTURE DOMAIN						
External network connectivity that affects interoperability	• (I1) Document the external interface connections	• Network Diagram	• SvcV-1 Services Context Description • SvcV-2 Services Resource Flow Description	• Provisioning Model		• Phase D: Technology Architecture
The standards at the infrastructure-external interface and technical standards profile	• (I2) List the technical standards that apply to services/solutions • (I3) List of emerging standards that need to be considered along with timeframes	• Technical Standards Profile • Technology Forecast	• StdV-1 Standards Profile • StdV-2 Standards Forecast	• Service Model	• Relevant Standard Matrix	• Environment and Location Diagrams • Platform Decomposition Diagram • Processing Diagram • Network Computing Hardware Diagram • Communications Engineering Diagram
SECURITY DOMAIN						
Assuring proper security controls are in place to ensure the protection of information as it is exchanged within and across security fabrics	• (S1) Show how the proper security controls are to be used to ensure data protection, as well as data access • (S2) Event trace can provide service/system details on interactions; only provide if more detail is needed as these take some time to develop	• Security Controls Catalog (Core) (SP-1) • Certification and Accreditation Documentation (SP-3)	• OV-5b: Operational Activity Model • SvcV-10c Services Event-Trace Description • DoD Information Assurance Accreditation Process	• Behavior Model • Service Policy and Service Contracts	• Same as DoDAF artifacts	• Preliminary Phase • Business Rules for Handling the Data and Information • Written and Published Security Policy • Codified Data Information Asset Ownership • Risk Analysis • Data Classification
Implement access authorization controls to protect shared data assets		• Security Controls Catalog (SP-1)	• DoD Information Assurance Accreditation Process	• Service Interfaces	• Uses DoDAF/UAF artifacts	• Disaster Recovery and Continuity Plans

APPENDIX C: INTEROPERABILITY MATURITY MODEL

The Interoperability Maturity Model of the ISE I^2F addresses the five domains of interoperability as defined in the FEAF. Each domain is supported by applicable questions and maturity model assessment criteria. Each row in the maturity models represents a functional area within the domain. Each column represents a different stage of maturity. Interdependencies between functional areas exist but the goal is to assess a system independently for each functional area.

C.1 BUSINESS DOMAIN INTEROPERABILITY OBJECTIVES

The purpose of the business domain is to ensure that the system, program or reference architecture aligns to an organization's mission requirements and clearly describes the scope, goals, and purpose of the architecture. The business domain typically describes:

- References to policies, guidance, and laws that affect the reference architecture and related mission objectives
- Governance groups responsible for oversight of the reference architecture
- Mission vision, objectives, and requirements
- Lines of business, capabilities, and activities
- Planned achievement of capabilities by timeframes and what constrains/policies apply

C.1.1 INTEROPERABILITY OBJECTIVES

Interoperability objectives of the business domain include:

- Description of how a reference architecture supports the operational enterprise
- Incorporating information sharing functions into mission-specific activities (e.g., address the information sharing lifecycle activities such as collection, analysis, dissemination, storage, and retirement)
- Using standards-based approaches to capture business requirements and document business processes and information flows
- Identifying common information exchanges for a specific mission scenario/use case
- Capturing information sharing requirements, constraints, and rules between partners

C.1.2 ASSESSMENT

The Business Domain maturity model is divided into functions or process groups (rows) and maturity levels (column). The maturity model is followed by several supporting questions.

	⓪ ABSENT ① AD HOC	② REPEATABLE	③ ENHANCED	④ MANAGED	⑤ OPTIMIZED
Business Process Definition	Formalized definitions of the business processes do not exist.	Definitions of the business processes are formalized and understood within the organization.	The formalized definitions of the business processes are understood by external partners.	Internal and external partners understand the various roles within the business process through manual workflows.	All internal and external partners understand the various roles within the business process through automated workflows. The business process definitions are improved as necessary through monitoring feedback from current processes and to better serve the organization's particular needs.
Business Process Models	Formalized business process models that describe the information sharing flows are not defined.	Business process models that describe the information sharing flows are defined by a modeling standard and are aligned to applicable policy, guidance, or law. The models employ repeatable exchange patterns.			The formalized business process models use a modeling standard (e.g., BPMN, WS-BPEL, IDEF0, or XPDL 2.1) and share and reuse processes. The models are available online to all authorized users.
Information Sharing Agreements (ISAs)	An ISA does not exist.	The ISA documents the purpose, scope, and authorized users of the data exchanges.	The ISA is understood by all users who are involved in the data exchanges and can be manually provided to authorized users.	The ISA is available online to authorized users and compliance is manually monitored.	Compliance to the ISA is automated. Metrics are collected and used to enhance interoperability across agencies.

C.2 DATA DOMAIN INTEROPERABILITY OBJECTIVE

The purpose of the data domain is to describe what data is available to promote the common identification, use, and appropriate sharing of data/information across the government. It provides guidance for consistently describing, categorizing, and sharing data, and facilitates the discovery and exchange of information across boundaries. It describes structure (logical and schema) of the data/information at a level necessary for users to understand both what types of data/information is available and the data's structure. The semantic meaning of the data/information should also be addressed within this domain in order to enable the interoperability of the data/information to be exchanged. This domain typically describes how:

- Data is classified within a given data source by the mission or business context in which the data is used
- Structured, semi-structured, and unstructured data is stored, managed, and used in a system
- Services and processes reference and manipulate data
- Business context is applied to data so that it can be searched
- Standardization of information exchange between information sharing partners

C.2.1 INTEROPERABILITY OBJECTIVES

Interoperability objectives of the data domain include:

- Describing how data is structured, what standards are used, how data/information can be exchanged so users are able to both have access to and use the data/information
- Specify/describe the data/information flow, including tagging, discovery, and retrieval of the data
- Demonstrating the commonly occurring need for exchanges of data/information between the domain and users
- Describing how data/information is secured throughout the lifecycle
- Specifying how data/information is tagged/structured, and how specific data tagging standards are used
- Describing principles, roles, and responsibilities for data management and stewardship

C.2.2 ASSESSMENT

The Data Domain maturity model is divided into functions or process groups (rows) and maturity levels (column). The maturity model is followed by several supporting questions.

	⓪ ABSENT	① AD HOC	② REPEATABLE	③ ENHANCED	④ MANAGED	⑤ OPTIMIZED
Data Exchange	—	Business context is applied to the data. Organization stores and manages defined, semi-defined, and undefined data for use by internal services and processes.		Data is exchanged across agencies and missions in a standardized way.		Data is exchanged across agencies and missions using open standards.
Structural Metadata Definitions	–	The data structure is defined.	Standards consistently define the data structure. Some automated data structuring and manual record-level tagging exists.	A consistent, agency-adopted format with mostly automated structuring and manual record-level tagging of the data exists.	Data tagging is semi-automated at the attribute-level with a community-adopted metadata format.	Smart data tagged at the attribute-level with open metadata standards.
Data Asset Discovery	Search capability does not exist.	Basic dataset-wide search capability exists.	Basic system-wide search. Business context is applied to the data so it is discoverable within the agency.	Basic search of data assets that is configurable to federate from any system using a specific agency-adopted service contract	Advanced search of data assets that is configurable to federate from any system using a community-adopted service contract.	Advanced search of data assets that is configurable to federate, is discoverable, available, and accessible across agencies and missions by using open standards
Exception Handling	The system is unable to store or process exceptions—received information that is inconsistent with internal information.	Exceptions are solely handled manually.		The system semi-automatically resolves the majority of exceptions.		The system automatically resolves the majority of exceptions.
Security and Privacy	Security achieved through isolation of systems and implementing current regulatory mandates or laws.		Supporting policies identified and under consideration.	Supporting policies in process of development and implementation.	Security is documented by consistent supporting policies, which are mostly implemented	Security is documented by consistent supporting policies, which are implemented.

C.3 APPLICATIONS AND SYSTEMS DOMAIN OBJECTIVES

The applications and systems domain describes the technical services supporting the common activities used for discovering, identifying, distributing, protecting, and managing the data/information that external users require. It should:

- Provide any applicable service standards, application architecture approaches (e.g., SOA), or other information required to interact with the applications/services within the domain
- Describe the relationships between systems, applications, and interfaces

C.3.1 INTEROPERABILITY OBJECTIVES

Interoperability objectives of the applications and systems domain include:

- Capturing the specifications and functional requirements of the applications/services to the level necessary so external application developers can interface with applications/services
- Describing recommended and/or possible implementation approaches (e.g., cloud, SOA, mobile)
- Identifying services and common activities, their service components, and the interfaces/interconnections between the services and data assets that are exchanged
- Identifying the functions performed by the applications/services and any constraints on the data used and the flow of the data
- Specifying service standards used or required by the applications/services
- Specifying rules/laws with respect to products, data, and/or information generated by the applications/services
- Publishing/exposing application programming interfaces (APIs) so future users can access and create applications with the data/information, and describing how the developers access the APIs
- Describing extensibility approaches for future users/applications to add additional functionality
- Describing how application architecture scales for more users
- Describing how services are made discoverable
- Specifying the provider and user roles and responsibilities with respect to application/service lifecycle (from development to operations and maintenance, to retirement)

C.3.2 ASSESSMENT

The Applications and Systems Domain maturity model is divided into functions or process groups (rows) and maturity levels (column). The maturity model is followed by several supporting questions.

	⓪ ABSENT	① AD HOC	② REPEATABLE	③ ENHANCED	④ MANAGED	⑤ OPTIMIZED
Business Service Models	Formalized business service models that depict information flows, relationships, and dependencies between services are not defined.		Business service models are defined by a modeling standard and are aligned to applicable policy, guidance, and laws. The models employ repeatable exchange patterns.			The formalized business service models are available online to authorized users
Service Discovery	Service is not discoverable	Service has undergone agency publication process, and is discoverable and accessible within the agency.		Service is discoverable and accessible by authorized users.		Service is discoverable and accessible by authorized external users through an online service registration and discovery mechanism.
Service Delivery Method	The data is not provided externally.	Data exchange occurs physically, by telephone, or by email	Data is exchanged by a system-specific service with mostly automated pushes and pulls.	Data is exchanged through an agency-wide service with entirely automated pushes and pulls.	The method of data exchange is configurable to operate with any system using a community-adopted proprietary format with entirely automated pushes and pulls.	The method of data exchange is configurable to operate with any system using an open standard with entirely automated pushes and pulls.
Service-Level Agreements (SLAs)	No SLA.			The SLA exists and includes requirements for service availability, serviceability, performance, operation, as well as the roles and responsibilities between the service provider and service consumer to deliver and maintain the service. Compliance of the SLA is not monitored.	The SLA includes the standard/ specification that addresses any interoperability considerations or constraints that affect implementation of the services. Compliance of the SLA is manually monitored.	The SLA includes the standard/ specification that addresses any interoperability considerations or constraints that affect implementation of the services. Compliance monitoring of the SLA is automated.

C.4 SECURITY DOMAIN INTEROPERABILITY OBJECTIVES

The purpose of security domain is to describe the security policies and considerations required for external users that need to interface and get access to the data/information. The Interoperability Maturity Matrix uses the **Federal Identity, Credential and Access Management (ICAM) Maturity Model** to assess the progress of an agency’s business processes and technical capabilities against the ICAM segment architecture, as related to interoperability within the security domain.[52]

C.4.1 INTEROPERABILITY OBJECTIVES

Interoperability objectives of the security domain include:

- Describing how proper security controls are used by the architecture to ensure data/information protection and allow access by external users
- Describing high-level security needs from an interoperability perspective, such as the use of common security standards/protocols
- Identifying controls required for specific types of information and any handling caveats (i.e., address confidentiality, integrity, and availability requirements)
- Describing how proper security controls are used to ensure data protection and ensure access
- Determining if information must be exchanged across different security enclaves
- Using metadata to tag data and describe its pedigree, lineage, source, timeliness, confidence, or other attributes associated with trust
- Identifying digital security rules, guidelines, and standards for securely exchanging data and services across security domains
- Describing, with enough detail for an external application developer, the event trace of the interactions of the architecture with regard to security controls
- Describing the identity management system used to allow/deny access to the data/information (i.e., role or attribute based)
- Describing the plan to manage/control your identity accounts and provide access controls to systems (for users, system administrators, developers, and super users)
- Describing how new users/developers are granted access to the data/information at all stages of the lifecycle
- Describing data/information access audit methods or standards, include the lifecycle for the storage of the audit data

[52] http://www.idmanagement.gov/documents/icam-maturity-model

C.5 PERFORMANCE DOMAIN INTEROPERABILITY OBJECTIVES

The purpose of the performance domain is to provide linkage to investments or activities and an organization’s strategic vision. This domain typically:

- Provides a direct line of sight between strategic planning and the investment review process
- Identifies common performance elements across investments or activities
- Provides a high-level overview of recommended metrics to be considered that will measure the successes of the architecture (inputs, outputs, and outcomes)

C.5.1 INTEROPERABILITY OBJECTIVES

Interoperability objectives of the performance domain include:

- Define performance goals that align to applicable policy, guidance and laws[53]
- Review investments and ensure they clearly incorporate interoperability requirements and adhere to relevant performance goals[54]

C.5.2 ASSESSMENT

The Performance Domain maturity model is divided into functions or process groups (rows) and maturity levels (column). The maturity model is followed by several supporting questions.

	⓪	①	②	③	④	⑤
	ABSENT	**AD HOC**	**REPEATABLE**	**ENHANCED**	**MANAGED**	**OPTIMIZED**
Metrics	Formalized performance metrics that provide direct line of sight between strategic planning and the investment review process do not exist.		Formalized performance metrics exist and align with strategic goals of organization as well as to applicable policy, guidance, and laws.	Formalized performance metrics that identify common performance elements across investments or activities exists.		Formalized performance metrics are used to inform gap analysis of interoperability requirements and adhere to relevant performance goals.

[53] Within the ISE, specific reference should be given to incorporating responsible information sharing goals and objectives as defined by the National Strategy for Information Sharing and Safeguarding.

[54] The ISE Performance Management Framework provides guidance on aligning vision, investment activities and metrics for responsible information sharing.

APPENDIX D:
ISE I^2F – REFERENCE ARCHITECTURE TEMPLATE

PURPOSE

The intent of the ISE I^2F Reference Architecture Template is to provide those building specific mission reference architectures with a mission agnostic approach that will result in an enhanced interoperable reference architecture which is specific to a mission when context is applied. In addition, this template can be used with existing reference architectures to plan for improving interoperability maturity based on the results of the Interoperability Maturity Model/Matrix in Appendix C. This mission agnostic approach is meant to provide key elements and concepts needed to be addressed to make these resulting architectures interoperable.

According to the DoD Reference Architecture Description[55] document, a common theme among the definitions is that the primary purpose of a Reference Architecture is to guide and constrain the instantiations of solution architectures. In addition, a Reference Architecture should:

- Provide common language for the various stakeholders;
- Provide consistency of implementation of technology to solve problems;
- Support the validation of solutions against proven Reference Architecture; and
- Encourage adherence to common standards, specifications, and patterns.

In general, a Reference Architecture is an authoritative source of information about a specific subject or mission area that guides and constrains the instantiations of multiple architectures and solutions.

STRUCTURE AND METHOD

The ISE Information Interoperability Reference Architecture Template provides the key elements, broken down by the Common Approach to Federal Enterprise Architecture domains: Business, Infrastructure, Data, Application/Service, Security, and Performance domains, to which the concepts of interoperability are applied.

HOW TO USE THIS TEMPLATE

The Common Approach is sub-divided into topic areas within each domain in order to further aid the reference architecture builders in bringing in the right resource expertise when needed. The

[55] http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf

elements and concepts spelled out are not meant to be exhaustive in nature but used as a guide in building out mission specific reference architectures to be more interoperable within their larger enterprises. In addition, mnemonics are used in this template that map back to the Architecture Framework Alignment Grid in Appendix B as an aid in generating the required architecture artifacts.

Each domain section has "Overview," "Objective of the Architecture," and "Key Focus Areas" explanation paragraphs that apply specifically to the domain section. The purpose of the paragraphs is to give guidance as to context to be focused on when developing the reference architectures within each of the domains.

The impetus of the template is the domain topic areas that contain elements and concepts to be considered when generating the mission specific reference architectures. The reference architect should approach each domain and examine how the listed elements and concepts apply to their specific mission context. In addition, please reference the Architecture Framework Mapping Grid using the mnemonics, included as an appendix this document, for further guidance on which artifacts to build using this template as guidance.

GETTING STARTED: REFERENCE ARCHITECTURE DEVELOPMENT

USING A COMMON APPROACH DOMAIN STRUCTURE

BUSINESS/MISSION DOMAIN SECTION

KEY FOCUS AREA
BUSINESS

Capture business requirements preferably using standards and guidance from organizations to develop diagrams, models and layers of abstractions to depict business analysis completed, business processes and organizational and business service relationships using standard methods (e.g., Business Process Model Notation (BPMN), IDEF0, Unified Modeling Language (UML), etc.). Services should be standardized both within and between agencies whenever possible to enhance interoperability. Standards Development Organizations should be primary source, i.e., IEEE, OMG, OASIS, NIST, and ISO, to enable the use of architecture and business models and analysis with regard to comparison or alternatives.

Alignment with ISE I^{2}F **Sections:** Section 3.1, Operational Capabilities; Section 3.4, Exchange Patterns.

Overview: Describe the lines of business and organizations and the operational concept to be achieved. Provide the overall vision in a strategic context for the capabilities and a high level scope. Provide a hierarchy of capabilities along with description of the capabilities. Show the planned achievement of the capabilities by time frames and what constrains/policies are being applied.

Objectives of the Architecture: Describe how the architecture supports the operational enterprise information/data and makes it discoverable/searchable, i.e., registry or service inventory. For example: The Identity and Access Management initiative provides enterprise information through the use of a global registry to support naming standards and federated access to support other mission capabilities.

Business Models, Diagrams, and Flows:

- Describe the operational concept to be achieved by the architecture and provide the overall vision in a strategic context for the capabilities. (B1)
- Describe the flow of resources/data exchanged from a business perspective between operational activities. (B6)
- General overview of architecture (description and graphics). (B2)
- Policy and Governance considerations: Provide policies, governance information, or applicable laws that will affect the implementation of the architecture. (B5)
- Architecture Environment considerations: Describe any federation, cloud, mobile considerations in the implementation of the architecture. (B5)
- Define the intended interoperability outcomes for each of the business functions within the architecture. (B4)

Business Processes:

- Establish specific exchange patterns for the architecture. (B6)
- Document internal and external information flows. (B6)
- Establish the authoritative sources of information/data along with agreements. (B7)
- Document any dependencies on other work not included in the reference.
- List assumptions used in development of the reference architecture.

Business/Mission Exchange Processes:

- Provide the exchange specification as they relate to the services which would include applicable technical standards from accepted standards bodies (e.g., ISO, IEEE, and NIST). (B9)
- Build use cases for each type of data exchange.
- Information/Data sharing access agreements established and exposed to users. (B8)

Other Business/Mission Domain Considerations:

- Consult security officer to capture applicable security rules/requirements. The results should be captured as annotations with the applicable artifacts
- Consult privacy officer to capture privacy rules/laws Applicable rules and laws should be noted on artifacts in order to capture them as requirements in the implementation lifecycle
- Consult the modernization plan to ensure alignment Modernization plan considerations should be captured on existing artifacts as discovered or as part of “to-be” artifacts

DATA DOMAIN SECTION

KEY FOCUS AREA

DATA

Capture the data considerations from how the data is structured, both logically and physically (if necessary), that enables users access to the data/information with enough specificity to be able to use the data/information. In order to enable interoperable solutions data and information exchanges should be based on open standards. Privacy considerations with respect to the data exchanges should be designed into every data solution. Capture any relationship between the data and business processes and any organizational or policy considerations that need to be addressed.

Alignment with ISE I^{2}F **Sections:** Section 3.1, Operational Capabilities; Section 3.2, Technical Standards; Section 3.3, Technical Capabilities; Section 3.4, Exchange Patterns; Section 3.6, Exchange Specifications

Overview: Describe what data is available to users and the structure (logical and schema) of the data/information at a level necessary for users to understand both what types of data/information is available and the structure of it.

Objective of the Architecture: Describe how the data domain is structured, what standards are used, how data/information can be exchanged, and the data lifecycle description in order for external users to be able to both have access and be able to use the data/information.

Data Considerations:

- Provide the high level data concepts and their logical entity relationships. (D1)
- Describe the data requirements and their relationships to the business process rules. (D2)
- Provide roles and responsibilities of the stakeholders involved with the data processes throughout the data lifecycle. (D4)
- Specify organizational relationships with respect to the data and its lifecycle. (D4)
- Describe the governance structure of the information/data throughout the data lifecycle. (D4)
- Describe the information/data management activities throughout the lifecycle. (D4)
- Specify any privacy restrictions on the information/data throughout the data lifecycle. (B6)

Data Interoperability Considerations:

- Describe the flow of resources/data exchanged in order to capture interoperability requirements. (B6)
- Describe how the information/data is secured throughout the lifecycle. (D3)
- Specify how the information/data is tagged/structured (standards used). (D5)
- Specify information exchanges and exchange format (e.g., NIEM). (D5)

- Specify the repeatable set of tasks that demonstrates the commonly occurring need for the exchange of data/information between the domain and users. (D3)
- Specify/describe the information/data flow to include the tagging of the data, discovery, and retrieval. (D3)

Data Standards and Exposure:

- Provide any necessary or relevant data standards to be considered for interoperability. (D5)
- Provide recommendation and/or constraints with regard to data standards within the architecture environment. (D5)

Information Sharing Agreements:

- Document the relevant information sharing agreements (ISAs) and how they affect the exchange of information between users. (D3)
- Provide a description of the business purpose of the information sharing agreements to include the roles and responsibilities of the data throughout the lifecycle. (D4)
- Provide measureable performance criteria for the data (e.g., storage, delivery, discovery, access requirements).

Other Data Domain Considerations:

- Consult security officer to capture applicable security rules/requirements. The results should be captured as annotations with the applicable artifacts.
- Consult privacy officer to capture privacy rules/laws. Applicable rules and laws should be noted on artifacts in order to capture them as requirements in the implementation lifecycle.
- Consult the modernization plan to ensure alignment. Modernization plan considerations should be captured on existing artifacts as discovered or as part of “to-be” artifacts.

APPLICATIONS AND SYSTEMS DOMAIN SECTION

KEY FOCUS AREA

APPLICATIONS AND SYSTEMS

Describe the applications/services and their interconnections between other services as well as the data assets and the information flows that are being used and exchanged. Applications/service and their external interfaces should be standardized when possible for scalability and interoperability purposes. Specify the service standards used and their applicability both internally, externally and reusability.

Alignment with ISE I^{2}F **Sections:** Section 3.1, Operational Capabilities; Section 3.2, Technical Standards; Section 3.3, Technical Capabilities; Section 3.4, Exchange Patterns; Section 3.6, Exchange Specifications.

Overview: Describe the technical services supporting the common activities used for discovering, identifying, distributing, protecting, and managing the data/ information needed by external users. Provide any applicable service standards, application architecture approaches such as SOA, or other information required to interact with the applications/service within the domain.

Objective of the Architecture: Capture the specifications and functional requirements of the applications/service to the level necessary for external application developers can interface with application/services available to externals.

Application/Service Environment Considerations:

- Identify services and common activities, their service component and the interfaces/ interconnections between the services and data assets that are exchanged. (A1)
- Describe recommended and/or possible implementation approaches (e.g., Cloud, SOA, Mobile) and considerations for approaches to be captured in applicable artifacts.
- Provide standards and/or standards requirements for consideration by the reference architecture. These need not be prescriptive but suggestive and currently utilized within the application class. (A6)
- Describe extensibility approaches for future users/applications in any modernization plan artifacts.
- Describe how the application architecture scales for more users in any modernization plan artifacts.

Application/Service Requirements/Constraints:

- Specify the standards/specifications used by the services to make them discoverable.
- Describe the functions performed by the applications/services and any constraints on the data used and the flow of the data. (A3)
- Describe the data assets used by the applications/services and how the data is exchanged between the services. (A2)

- Describe the data flows being exchanged between services and the attributes of the exchanges. (A4)
- Specify any service standards used by or required by the applications/services. (A6)
- Specify how the "service-level agreements" are enforced (manually or machine-level) and the standard/specification if machine-level. (A6)

Application/Service Provider and User Roles and Responsibilities:

- Specify the provider and user roles and responsibilities with respect to application/service lifecycle (Development – O&M – Retirement). (B4)
- Specify rules/laws with respect to products/data/information generated by the applications/services. (A5)

API Considerations:

- APIs published/exposed so that future users can access and create applications with the information/data, describe how the developers access the APIs. (A6)

Cloud Application/Service Implementation Considerations:

- Describe 'continuity of operations' considerations for information/data flows. (A3)

Mobile Application/Service Implementation Considerations:

- Describe mobile implementation considerations that are unique to the mobile architecture environment in addition to service identification. (A1)

INFRASTRUCTURE DOMAIN SECTION

KEY FOCUS AREA

INFRASTRUCTURE

Capture the interface requirements to the level needed to facilitate interoperability between systems as well as specifying the specific standards used by the interfaces, networks, and platforms that we exposed to externals. In addition, use well documented interfaces built on non-proprietary open platforms using standard platform independent data protocols. Host solutions must be compliant with current federal, state, and local policy and standards. Technology convergence that supports infrastructure consolidation should be pursued wherever possible. Describe any network specifications required by external systems in order to exchange data/information and be able to use it.

Alignment with ISE I^{2}F **Sections:** Section 3.3, Technical Capabilities

Overview: Describe what types of voice, data, mobile, and video networks will be required to host the IT systems/applications and to transport associate, data, images, and conversations, as well as "what type of physical infrastructure is needed to support the networks" (e.g., buildings, server rooms, points of presence, and other equipment).

Objective of the Architecture: Describe the infrastructure interfaces, i.e., protocols, and interface standards, and networks making external domains and applications/ services interoperable.

Infrastructure Interfaces:

- Document physical and logical interfaces. (I1)
- Describe interfaces from an architecture perspective. (I1)
- Describe infrastructure performance requirements. (I1)

Interface Standards:

- Specify any technical standards required or recommended for the architecture. (I2)
- Provide a list of emerging standards that need to be considered along with application timeframes. (I2)

Network Considerations:

Specify any network category and considerations or standards for each of the fabrics listed below:

- SBU
- Secret
- Top Secret

SECURITY DOMAIN SECTION

KEY FOCUS AREA

SECURITY

Provide the activities required demonstrating the flow of security information and security controls allowing external users and applications/services access to data assets. Security controls with respect to interoperability should be considered up front for every technology solution. Consider how security controls affect business services and information flows as well as the design and operation of systems, services, and networks. Provide any security constraints such as required security standards used by the architecture.

Alignment with ISE I^{2}F **Sections:** Section 3.1, Operational Capabilities; Section 3.2, Technical Standards; Section 3.3, Technical Capabilities; Section 3.4, Exchange Patterns; Section 3.6, Exchange Specifications

Overview: Describe the security policies and considerations required of the architecture that external users will need to interface and get access to the data/information. Provide the necessary security controls to ensure the protection of data/information as it is exchanged within and across security fabrics.

Objective of the Architecture: Describe how the proper security controls are to be used by the architecture to ensure data/information protection and allowing access by externals.

General Security Considerations:

- Describe high-level security needs from an interoperability perspective such as the use of common security standards/protocols.
- Describe how proper security controls are to be used to ensure data protection and ensure data access. (S1)
- Describe the event trace of the interactions of the architecture with regard to security controls. (S2)

Security Interoperability Considerations:

- Describe the identity management system used to allow/deny access to the information/data. Role or attribute based?
- Describe the plan to manage/control your identity accounts and provide access controls to systems (for users, system admins, developers, “super users”).
- Describe how new user/developers are granted access to the information/data at all stages of the lifecycle.
- Describe information/data access audit method or standard, include the lifecycle for the storage of the audit data.

Other Security Domain Considerations:

- Consult security officer to capture applicable security rules/requirements. The results should be captured as annotations with the applicable artifacts.
- Consult privacy officer to capture privacy rules/laws. Applicable rules and laws should be noted on artifacts in order to capture them as requirements in the implementation lifecycle.
- Consult the modernization plan to ensure alignment. Modernization plan considerations should be captured on existing artifacts as discovered or as part of "to-be" artifacts.

PERFORMANCE DOMAIN SECTION

KEY FOCUS AREA

PERFORMANCE

Provide metrics by which to measure and architecture's interoperability within and between agencies and levels of government. Metrics could include: percentage of open standards adopted and used by systems in the architecture; percentage of applications /services designed to operate in the cloud or web-enabled. If possible specify how each element of the architecture contributes to the overall goal of interoperability both internally and externally to the architecture. Describe the relationship between investments and their alignment with interoperability goals and how to measure the effectiveness of the investments.

Alignment with ISE I^{2}F **Sections:** Section 3.1, Operational Capabilities

Overview: Describe the metrics necessary to determine whether the implementation of the architecture is successful. Describe also how the metrics will determine the utility of the resulting architecture.

Objective of the Architecture: Provide metrics to be used to measure quantitatively how well the architecture is performing and/or how interoperable, as measured by the interoperability requirements within the ISE I^{2}F.

Architecture Interoperability Performance Considerations:

- Provide a high-level overview of recommended metrics to be considered that will measure the successes of the architecture.
- Review OMB mandated Exhibit 53 and 300 requirements (applies to federal only) and consider how to show the investments contribution to the architecture's interoperability targets.

Interoperability Performance Metrics:

Provide metrics by which the architecture's performance can be measured from an interoperability perspective and how will the performance be reported. These metrics should aid in deriving the eventual performance requirements of the reference architecture's underlying systems.

APPENDIX E: EXCHANGE PATTERNS – USE CASE 1

NATIONAL VIRTUAL POINTER SYSTEM

PURPOSE

A use case defines a sequence of actions that yields an observable result of value. Use cases provide a structure to express functional requirements within the context of mission/business and system processes. Use cases can be represented graphically or in a textual document.[56]

This use case example describes how the ISE I^{2}F can be applied to a specific mission-oriented scenario to document interoperability requirements. Use cases can be a valuable tool in verifying interoperability as they may yield repeatable actions or behaviors that can be in made into patterns. These patterns may be candidates for standardization, which will both enrich and simplify interoperability (i.e., data and information exchange).

The following use case example applies the ISE I^{2}F to the National Virtual Pointer System (NVPS) against six partitions: operational capabilities, exchange patterns, exchange profiles, exchange specifications, technical standards, and technical capabilities.

SCENARIO BACKGROUND

In an effort to identify investigative overlaps, increase efficiency and officer safety, Regional Information Sharing Systems (RISS) centers and High Intensity Drug Trafficking Areas (HIDTAs), in partnership with the Drug Enforcement Administration (DEA), the International Justice and Public Safety Network (Nlets), and the National Alliance of State Drug Enforcement Agencies (NASDEA) developed the National Virtual Pointer System[57] to connect law enforcement officers who may be investigating the same or related cases.

NVPS is a system that connects multiple existing investigative target deconfliction databases by granting access to participating federal, state, local, and tribal law enforcement agencies through any one of the participating systems. Once agents and officers enter the subjects of their current investigations into their target deconfliction database, the system automatically notifies them if another NVPS participant is investigating the same target.[58] The systems do not directly communicate with each other but are connected to the NVPS message hub, which validates and

[56] http://pic.dhe.ibm.com/infocenter/rpcmpose/v2r0/index.jsp?topic=/com.ibm.rational.rrc.help.doc/topics/c_uc.html
[57] http://www.gao.gov/assets/660/653527.pdf, pg 31.
[58] http://www.ncirc.gov/documents/public/supplementaries/law_enforcement_intelligence.pdf, pg 89.

routes data if the mandatory minimal data elements are submitted as part of the target deconfliction database entry.

SCENARIO PARTICIPANTS

ORGANIZATION	INFORMATION SHARING NETWORK
Junction City, KS Police Department	Local databases and the Kansas State Intelligence System (available via RISSNET)
Kansas City DEA Interdiction Task Force	DEA NDPIX entry via DOJ Network routed to the NVPS Message Hub via Nlets and RISSNET.
DEA New Jersey Field Office	DEA NDPIX notification via DOJ Network routed from the NVPS Message Hub via Nlets and RISSNET.

SCENARIO STEPS

1. A Junction City, Kansas police officer arrested a suspect for dealing methamphetamine. A check of local record databases and the Kansas State Intelligence System provides no matching information. The investigation however shows drug movement through the Kansas City International Airport and contact is made with the airport interdiction team.
2. Agent A of the Kansas City Drug Enforcement Administration Interdiction Task Force was assigned to the case.
3. Agent A enters her contact information and the suspect's basic data into the National Drug Pointer Index (NDPIX). As an NVPS participant, the record entry automatically spawns an NVPS query to all NVPS participants
4. The record travels through encrypted tunnels from the DOJ network to the NVPS message hub over two proprietary intranets: RISSNET secure intranet and Nlets.5. The NVPS message hub proxies the message and launches queries to all participating deconfliction systems.
6. The NVPS message hub receives pointer index information from another deconfliction system, indicating a matching case involving the suspect.
7. The NVPS message hub sends a message to the originating system indicating the match and how to contact the other investigating agency. The message shows up as notifications on the originating system.
8. Simultaneously, another NVPS message is generated and sent to Agent B at the DEA New Jersey Field Division (Targeted deconfliction system) alerting him of the Kansas City inquiry.
9. Once notifications are reviewed, they are not stored on the NVPS message hub.

10. Coordinating between the Junction City Police Department, the Kansas City DEA Interdiction Task Force, and the New Jersey Field Division resulted in the identification of additional members of the drug trafficking organization and subsequent arrests.[59]

ISE I^{2}F CONCEPTS APPLIED

OPERATIONAL CAPABILITIES

For this use case, the Operational Capabilities statement is: “The NVPS operational capabilities enable law enforcement officers to engage in target deconfliction with officers across the country.”

Please see Section 3.1 for more information on operational capabilities.

TECHNICAL CAPABILITIES

Technical capabilities used in this NVPS scenario include:

- Discovery
- Messaging
- Collaboration
- Storage

Note: All applications and systems accessed in the scenario utilized the following capabilities:

- Security
- Auditing
- Mediation
- Enterprise Service Management

Please see Section 3.2 for more information on technical capabilities.

TECHNICAL STANDARDS

Technical standards used in this NVPS scenario include:

- NVPS message: Built to GJXDM 3.0.3.
- NLETS message: Built to GJXDM-compliant format.
- NDPIX message: Built as text-based parsed format.

[59] http://www.statetechmagazine.com/article/2007/09/pointing-the-way

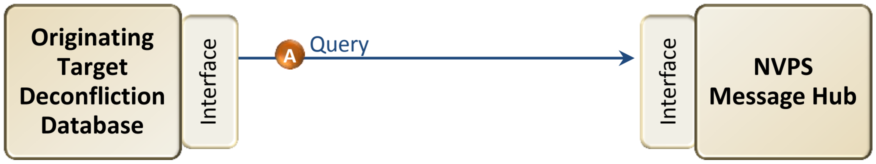
Please see Section 3.3 for more information on technical standards.

EXCHANGE PATTERNS

The following exchange patterns identify the basic types of message exchanges within the NVPS use case scenario, and reflect what content should be included in the ISE common profile description for the exchange patterns.

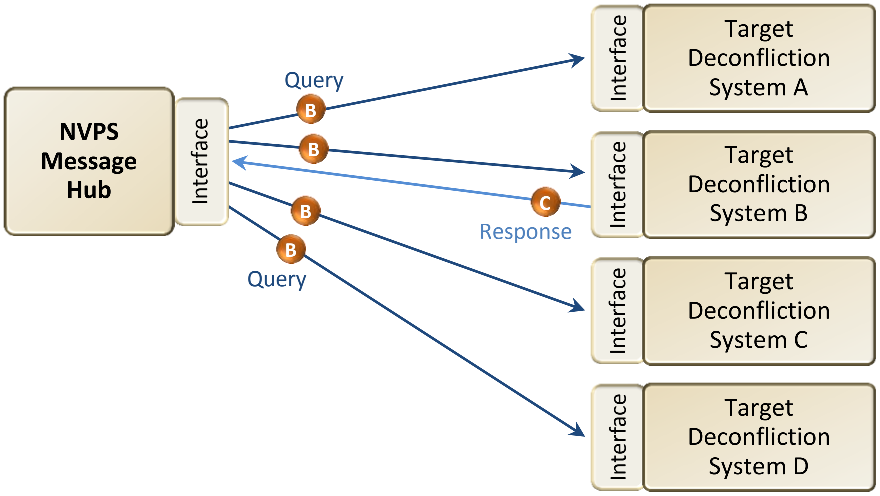
Please see Section 3.4 for more information on exchange patterns.

A. The originating system creates a target record for deconfliction which is routed to the NVPS message hub.

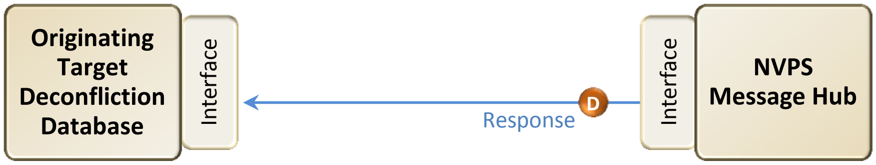


B. The NVPS message hub routes the target record for **Query** to the interfaces of connected target deconfliction systems.

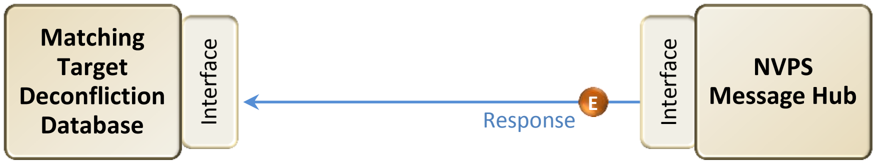
C. Target deconfliction system B **responds** to the NVPS message hub's query with pointer index information of a matching case.


NVPS Message Hub
Interface
Query
B
B
B
B
Query
C
Response
Interface
Target Deconfliction System A
Interface
Target Deconfliction System B
Interface
Target Deconfliction System C
Interface
Target Deconfliction System D

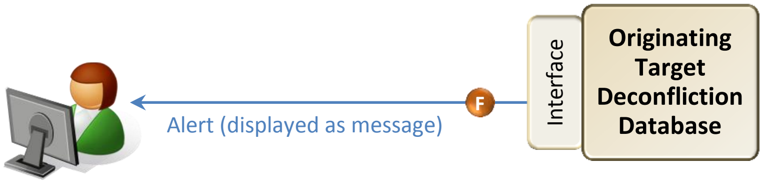
D. The NVPS message hub routes the **response**, which includes the point of contact information for the matching case, to the originating system.



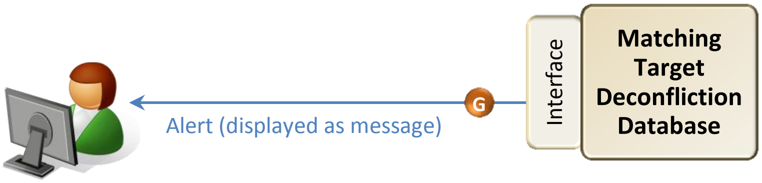
E. The NVPS message hub also routes the **response** to the matching entity.



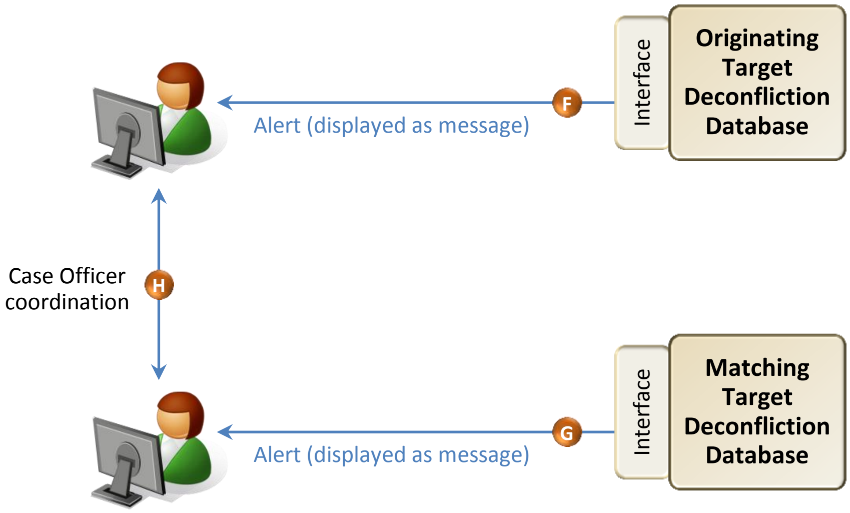
F. The originating system and matching system receives a notification **Alert** and displays it as a message.


Alert (displayed as message)
F
Interface
Originating Target Deconfliction Database

G. The matching system receives a notification Alert and displays it as a message.


Alert (displayed as message)
G
Interface
Matching Target Deconfliction Database

H. The originating and matching case officers contact each other and share investigative details as appropriate.


Originating Target Deconfliction Database
Interface
F
Alert (displayed as message)
Case Officer coordination
H
Matching Target Deconfliction Database
Interface
G
Alert (displayed as message)

EXCHANGE PROFILES

For each topic identified below, the question posed describes what content to provide for the related exchange profile sub-section.

- **Process:** What business process allowed this scenario to occur?
- Participants agreed to required and optional data elements, exchange methodology, and use of message hub as broker.
- **Data:** What is exchanged?
- Basic officer, agency, and target information. There are required and optional data elements. The optional data elements are just other identifying data about the target.
- **Services:** How is information shared (e.g., XML, Web Service-based system)?
- XML based web service using GJXDM3, Nlets XML, and NDPIX text format
- **Policy:** What are the terms and conditions that allow this scenario to occur?
- NVPS Policy and Technical requirements established by the NVPS Coordinating Committee (NVPS CC) and the NVPS Technical Working Group (NVPS TWG).

Please see Section 3.4.6 for more information on exchange profiles.

EXCHANGE SPECIFICATIONS

These are the rules for exchange of information used in the NVPS. These requirements are developed by the participants and users of the systems and information.

Please see Section 3.5 for more information on exchange specifications.

APPENDIX F: AUTHORITIES AND REFERENCES

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), as amended, establishes the ISE and lists a series of attributes required of the ISE to ensure that it "provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, tribal, and territorial entities, and the private sector through the use of policy guidelines and technologies."[60] It provides the duties and responsibilities of the PM-ISE and those of "the head of each department and agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE." Agencies are directed to:

- Ensure full department or agency compliance with information sharing policies, procedures, guidelines, or rules, and standards established in IRTPA 1016(b) and (f);
- Ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;
- Ensure full department or agency cooperation in the development of the ISE to implement government-wide information sharing; and
- Submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, directs agencies when preparing terrorism information for maximum distribution to use "the common standards for the sharing of terrorism information," as appropriate, in carrying out IRTPA Section 1016.[61]

Presidential Memorandum, Guidelines and Requirements in Support of the Information Sharing Environment, dated December 16, 2005, states that "the ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE."[62] Presidential Memorandum, Assignment of Functions Relating to the Information Sharing Environment, dated April 10, 2007, directs the Director of National Intelligence to ensure that the program manager responsible for information sharing across the Federal Government, pursuant to IRTPA Section 1016(b), be the assistant to the Director in carrying out the functions delegated in the memorandum. Circular A-130, which establishes policy for the management of Federal information resources, states that agencies will conduct information management planning using

[60] http://ise.gov/intelligence-reform-and-terrorism-prevention-act-2004-sec-1016-information-sharing
[61] http://ise.gov/intelligence-reform-and-terrorism-prevention-act-2004-sec-1016-information-sharing
[62] http://ise.gov/sites/default/files/Memo_on_Guidelines_and_Rqmts_in_Support_of_the_ISE.pdf

"voluntary standards and Federal Information Processing Standards where appropriate or required."[63]

The Information Sharing Access Interagency Policy Committee (ISA IPC), empowered by Presidential Policy Directive 1 (PPD-1), is the primary body for interagency coordination of national security policy. IRTPA Section 1016(g) directs agencies to contribute to this governance process. The ISA IPC subcommittees and working groups include representatives of state, local, tribal, and territorial governments, and industry.

ISE guidelines and policies impact the manner in which mission partners share and safeguard information, which necessitates mission partners to coordinate their information sharing and safeguarding activities. If appropriately coordinated through White House leadership, the Office of Management and Budget (OMB), and other authorities, the ISE will achieve broader information sharing success.

F.1 DRIVERS AND REQUIREMENTS

The ISE Drivers and Requirements Document[64] describes the authoritative mandates (e.g., Executive Orders, Public Laws) that direct the ISE. These ISE drivers and requirements are strategic in nature and establish direction to bring about ISE-specific results.

The Presidential Guidelines direct that "the ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively 'resources') used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information."[65] This Presidential direction resulted in the PM-ISE developing architectural framework and standards documentation to further define the ISE-specific drivers and requirements. This ISE documentation will facilitate information sharing practices, reduce barriers to sharing, and institutionalize sharing by providing a new construct for planning, installing, and operating nationwide information resources within the fabric of the ISE.

Federal agencies are responsible for aligning to strategies and guidance that impact the strategic direction of agency-level target architectures. Current government architecture and guidance memoranda include:

- The National Strategy for Information Sharing and Safeguarding (NSISS)[66], which was signed by the President on December 19, 2012. This new National Strategy is part of a

[63] http://www.whitehouse.gov/omb/circulars_a130_a130trans4
[64] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf
[65] http://www.ise.gov/background-and-authorities
[66] http://ise.gov/sites/default/files/2012infosharingstrategy.pdf

policy continuum that includes IRTPA Section 1016, the 2007 National Strategy for Information Sharing, Executive Orders 13587 and 13388, the ISE Presidential Guidelines, and the National Security Strategy.

- The Federal Information Technology (IT) Shared Services Strategy (Shared-First) released by the OMB to provide Federal agency chief information officers (CIOs) and key stakeholders guidance on the implementation of shared IT services as a key part of their efforts to eliminate waste and duplication and reinvest in innovative mission systems.
- The Common Approach to Federal Enterprise Architecture (Common Approach), which supports Shared-First, is "a guidance document for a common approach to the practice of Enterprise Architecture (EA) throughout the Executive Branch of the U.S. Federal Government."[67] The Common Approach promotes agencies ensuring "that EA solutions conform to Federal-wide standards whenever possible" to improve interoperability between agencies and with external stakeholders.

F.2 POLICY AND GOVERNANCE

F.2.1 ANNUAL LIFECYCLE AND REPORTING

To accurately report progress on the extent to which the ISE has been implemented, PM-ISE uses inputs from the ISE Annual Performance Assessment Questionnaire, which is issued to ISE departments and agencies; solicited inputs from the ISE governance bodies that define goals for and monitor the progress of ISE mission partners; and solicited descriptions of accomplishments from all mission partners, federal and non-federal, to ensure the best possible representation of the state of the ISE and information sharing across the enterprise. In addition, PM-ISE leverages data collected by the OMB to determine the extent to which ISE priorities are being incorporated into agency IT budgets.

Since January 2011, ISA IPC sub-committees and working groups have organized and managed their efforts, and report their accomplishments on a quarterly basis in line with annual and longer-term objectives and goals for the ISE. The sub-committees and working groups derive these key objectives and areas of responsibility in the form of concrete goals aligned to the mission needs as specified in the annual ISE programmatic guidance, the National Strategy for Information Sharing, and priorities specified by the administration.

F.2.2 PROGRAM AND IMPLEMENTATION GUIDANCE

The national security of the United States hinges on responsible and timely sharing of a vital national asset—information. Information sharing to protect the American people is a top priority

[67] Office of Management and Budget, *A Common Approach to Federal Enterprise Architecture*, May 2012. https://cio.gov/wp-content/uploads/downloads/2012/09/Common_Approach_to_Federal_EA.pdf

of the President. Since last year's annual report[68], the President issued the National Strategy for Information Sharing and Safeguarding. The new National Strategy serves as a guide for collective government efforts that promote responsible information sharing and safeguarding in support of our national security. Many of the goals and objectives reflect work already underway in our office and across the government. The ISE is acting on the leadership provided in the National Strategy to advance responsible information sharing efforts nationwide.

The focus of the FY 2015 ISE Implementation Guidance—PM-ISE, in collaboration with the ISA IPC, annually issues Implementation Guidance that is sequentially derived from and reinforces White House programmatic guidance—is geared toward implementing plans to realize the goals and objectives of the National Strategy, and it is structured around the National Strategy priority objectives. Further, the Implementation Guidance contains actions assigned to specific federal agencies, with milestones and timeframes, aligning programs, systems, and initiatives with requirements to improve responsible information sharing. Annual performance assessments against these actions provide accountability and progress over time, enabling leadership to make informed program and budget decisions in subsequent years. Overall, the annual planning cycle moves agencies closer to the target vision of responsible information sharing.

[68] http://www.ise.gov/annual-report

APPENDIX G: GLOSSARY

The ISE Building Blocks website Glossary contains an extensive list of all terms. The following terms are found within this document:

Capabilities: Mission partners and stakeholders have automated computer software-based information systems *capabilities* that they provide to one another. These capabilities "solve or support a solution for the problems [businesses] face in the course of their business." That is, capabilities are the things organizations have to solve problems and therefore add value, directly or indirectly, to their stakeholders.

Service: A *service* is the way in which one entity gains access to a capability offered by another entity.

Service Provider: A *service provider* is an entity (person or organization) that offers the use of capabilities by means of a service.

Service Consumer: A *service consumer* is an entity that seeks to satisfy a particular need through the use of capabilities offered by means of a service.

Service Broker: A *service broker* or intermediary is any capability that receives messages from a consumer and subsequently, as a service consumer itself, interacts with another service. The term "intermediary" indicates that these capabilities sit between other services and "mediate" the interaction by managing, controlling, brokering, or facilitating the transmission of messages between them.

Service Interface: A *service interface* "is the means for interacting with a service. It includes the specific protocols, commands, and information exchange by which actions are initiated [on the service]." A service interface is what a system designer or implementer (programmer) uses to design or build executable software that interacts with the service. That is, the service interface represents the "how" of interaction.

Pattern: A pattern, within the context of this document, is a general, repeatable set of tasks that help accomplish the commonly occurring need for exchange of data or information between two or more exchanging partners.

Message: A *message* is defined as the entire "package" of information sent between service consumer and service (or vice versa), even if there is a logical partitioning of the message into segments or sections. For instance, if an interface expresses actions as operations or functions that take arguments, and a particular operation has two arguments, both arguments would be considered part of the same message, even though they may be logically separated within the message structure. A message also includes the concept of an "attachment," in which there are several additional sections (attachments) that relate to a distinct, "primary" section.

APPENDIX H: ACRONYMS

The ISE Building Blocks website Glossary contains an extensive list of acronyms and terms. The following acronyms are found within this document:

AM	Administrative Memoranda
ANSI	American National Standards Institute
API	Application Programming Interface
BPEL	Business Process Execution Language
BPMN	Business Process Modeling Notation
CA	Common Approach
CIO	Chief Information Officer
CIOC	Chief Information Officers Council
Cir	Circular
CRM	Consolidated Reference Model
CUI	Controlled Unclassified Information
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DEA	Drug Enforcement Administration
EA	Enterprise Architecture
EAMM	Enterprise Architecture Maturity Model
ECM	Enterprise Competency Model
ESL	Enterprise Services List
FCIOC	Federal Chief Information Officer Council
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FICAM	Federal Identity, Credential, and Access Management
FSLTT	Federal, State, Local, Tribal, and Territorial
GFIPM	Global Federated Identity and Privilege Management
GJXDM	Global Justice XML Data Model
GML	Geospatial Markup Language
GRA	Global Reference Architecture
HIDTA	High Intensity Drug Trafficking Area

IL	Integrated Landscape
IC ITE	Intelligence Community Information Technology Enterprise
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
ICEA	Intelligence Community Enterprise Architecture
IDEF0	ICAM Definition for Function Modeling
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEPD	Information Exchange Package Documentation (NIEM)
IP	Internet Protocol
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA IPC	Information Sharing and Access Inter-agency Policy Committee
ISA	Information Sharing Agreement
ISE	Information Sharing Environment
ISO	International Organization for Standardization
IT	Information Technology
MDA	Maritime Domain Awareness
MOU	Memorandum of Understanding
MQ	Message Queue
NASDEA	National Alliance of State Drug Enforcement Agencies
NDPIX	National Drug Pointer Index
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NSI	National Suspicious Activity Reporting (SAR) Initiative
NSISS	National Strategy for Information Sharing and Safeguarding
NVPS	National Virtual Pointer System
OASIS	Organization for the Advancement of Structured Information Standards
OMB	Office of Management and Budget
OMG	Object Management Group
OSI	Open Systems Interconnection
QoS	Quality of Service
PAG	Program Architecture Guide
PKI	Public Key Infrastructure
PM-ISE	Program Manager, Information Sharing Environment

PMO	Program Management Office
PPD	Presidential Policy Directive
RA	Reference Architecture
RESTful	Representational State Transfer
RISS	Regional Information Sharing Systems
SAML	Security Assertion Markup Language
SAR	Suspicious Activity Reporting
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SDO	Standards Development Organization
SLA	Service-level Agreement
SLT	State, Local, and Tribal
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SP	Special Publication
TG	Technical Guidance
TOGAF	The Open Group Architecture Framework
TST	Technical Services Taxonomy
TTX	Tabletop Exercise
TWG	Technical Working Group
UML	Unified Modeling Language
VOIP	Voice Over Internet Protocol
WS*	Web Services Specifications
W3C	World Wide Web Consortium
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language

This page intentionally left blank.

Program Manager, Information Sharing Environment
Washington, D.C. 20511

202.331.2490

www.ise.gov

@shareandprotect

fb.me/informationsharingenvironment

http://lnkd.in/zaCB97

youtube.com/shareandprotect

ise.gov/blog

ise.gov/email